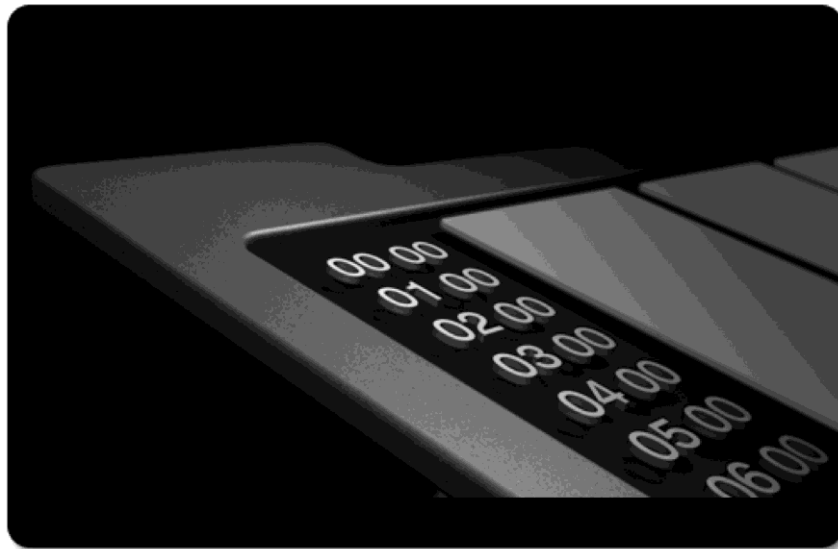


Display Content Manager

Digital Signage Management System



Installation Guide

Software Version 1.80

www.mediaedge-corp.com

Display Content Manager Installation Guide

Install & Setup

Display Content Manager
Installation Guide
Aug. 1, 2013

Copyright © 2013 MEDIAEDGE Corporation

Precautions when using this product

The precautions that are required when using Display Content Manager are described below. If you do not understand anything about the usage methods or related information, or if you have any queries, please contact the dealer where you purchased the product.

Cautions

1. It is prohibited to copy without permission, in whole or in part, this product (= Display Content Manager software) and all related products, including the manual that comes with the product and the other supplied items.
2. The configuration and specifications of this product may be changed in the future without prior notice.
3. Every effort has been made to develop the best possible product configuration, but should you notice something unusual, defects or anything else that concerns you, please contact the dealer where you purchased the product.
4. Regardless of item 3, we take no responsibility for any issues resulting from the running of this product.
5. Regardless of whether or not there was negligence during use, we take no responsibility whatsoever for special, attendant or consequential damages, including lost earnings, that arise from running this product, or for claims regarding such damages.
6. It is prohibited to analyze, reverse engineer, decompile or disassemble the software and hardware that are included with this product and all related products, including the other supplied items.
7. Microsoft, Windows and Internet Explorer are registered trademarks of the USA Microsoft Corporation. Other product names and related terms are the trademarks or registered trademarks of the corresponding companies.

About descriptions in this manual

- The Display Content Manager Installation Guide (this manual) describes the product configuration of Display Content Manager Ver.1.80 (As of June, 2013).
- The information in this manual is stored as a Readme file on the disk that is supplied with the product. Be sure to read this manual before using the product.
 - You can open the file by selecting [Start]-[All Programs]-[MEDIAEDGE]-[Display Content Manager]-[Readme].
- If there are any difference between the descriptions in Display Content Manager Installation Guide and the actual operation methods, give priority to the actual operation methods.
- To make the descriptions in the manual easier to understand, the illustrations or screenshots may differ from the actual product.
- Display Content Manager Installation Guide is aimed at people who can already perform basic computer operations. Operations not described in this manual are the same as normal computer operations.

Warnings

- Health precautions
In very rare cases, bright light stimulation or flashing on computer monitors or television screens may induce temporary epilepsy or loss of consciousness. Even people who have never experienced this before may be vulnerable to such reactions. People who have had such experiences or people with blood relatives who have had such experiences must consult a doctor before using this product.
- About copyright law and other legal responsibilities for use Any recordings made using this product are the responsibility of the user, and we take no responsibility whatsoever for any issues that may arise under copyright law, personal information protection law, or any other regulations.
- Regarding the handling of computers Be careful of the following regarding the handling of server computers and other computers on which Display Content Manager is installed.
 - ✧ Do not damage the power cord (or the AC adapter for notebook computers)
 - ✧ If you damage the power cord or AC adapter of a computer, it may cause a fire or electric shock. Do not place heavy objects on the cord or use it near heating devices. Do not fold back the power cord or modify it. Also, when disconnecting the power cord, hold it by the plug area. If the power cord is damaged, contact the dealer where you purchased the product for a replacement.
 - ✧ Do not open the case
 - ✧ If you open the case of the computer or try to modify it, it may cause a fire or electric shock. For internal inspection or repair, contact the dealer where you purchased the product.
 - ✧ Do not use the computer in a dusty or humid location
 - ✧ A short circuit or heat generation may occur and cause a fire or electric shock.
 - ✧ Do not let water or foreign matter inside
 - ✧ If water or foreign matter gets inside the computer, it may cause a fire or electric shock. Should water or foreign matter accidentally get inside, turn off the power to the device, disconnect the power cord or AC adapter from the outlet, and contact the dealer where you purchased the product.
 - ✧ Do not use during a thunderstorm
 - ✧ Do not touch the main computer unit or the plug. Doing so may cause an electric shock.
 - ✧ Do not touch the power cord or AC adapter with wet hands
 - ✧ Do not disconnect or insert the power cord or AC adapter of the computer with wet hands. Doing so may cause an electric shock.
 - ✧ Do not place in a location exposed to direct sunlight
 - ✧ Do not place the computer in a location exposed to direct sunlight or next to heating devices. Doing so may cause a fire or product malfunction.
 - ✧ Do not use if smoke appears
 - ✧ Do not use the computer in an abnormal condition, such as when smoke appears from it or if there is an abnormal odor. Doing so may cause a fire or product malfunction. Should an abnormality occur, turn off the power to the computer, disconnect the power cord or AC adapter, make sure that the smoke stops, and then contact the dealer where you purchased the product.
 - ✧ Do not place in an unstable location
 - ✧ Do not place the computer on an unstable stand or in a sloping location. It may fall and cause an injury or malfunction.
 - ✧ Turn off the power before cleaning
 - ✧ Before connecting or cleaning the product, disconnect the power cord or AC adapter. Otherwise, it may cause an electric shock or product malfunction. Do not use volatile solvents such as thinners when cleaning.
 - ✧ Do not use non-specified power cords or AC adapters

- ✧ Do not use power cords or AC adapters other than those that are supplied with the computer. Doing so may cause a fire or product malfunction.
- ✧ Lay out the cords correctly
- ✧ Lay out the power cord, AC adapter and AV cables in an organized manner. If someone trips over a cord, it may cause an injury or product malfunction.
- ✧ Do not cover the computer with a cloth
- ✧ Do not use the computer in a poorly ventilated location or while it is covered by a cloth or something similar. If the vents are blocked, heat will build up inside and may cause a fire or product malfunction.
- ✧ If you will not use the product for a long time, disconnect the power cord or AC adapter
- ✧ For safety, when you are not using the product, disconnect the power cord or AC adapter of the computer from the outlet.

INDEX

I. Checks	12
I-1. Overview of Display Content Manager	13
I-2. Overview of the DCM Application	14
I-3. System Components.....	15
I-3-1. Operation PC	15
I-3-2. DCM server.....	15
I-3-3. FTP server.....	16
I-3-4. MEDIAEDGE-SVS server	16
I-3-5. Playback clients	17
I-3-6. Network	18
I-4. System Configuration	19
I-4-1. Smallest configuration without using a server	20
I-4-2. Configuration using a DCM server	21
I-4-3. Configuration using one MEDIAEDGE-SVS server	22
I-4-4. Configuration using multiple MEDIAEDGE servers	23
I-4-5. Large-scale configuration that separates all server functions	25
I-4-6. Configuration that delivers contents via the Internet	27
II. Setup	28
II-1. Network Settings	29
II-2. Display Content Manager Installation.....	30
II-2-1. DCM server and DCM application installation	30
II-2-2. DCM application installation	34
II-2-3. DCM server, DCM add-on for SVS and DCM application installation.....	37
II-3. DCM Config Tool	41
II-3-1. DataBase Connection.....	41
II-3-2. Server Conenction.....	42
II-4. MEDIAEDGE-SVS Server Installation.....	43
II-4-1. SVS4 installation	43
II-5. Display Content Manager Version Upgrade.....	49
II-6. To secure the DCM system	51
II-6-1. Change the MeDcmUser's password	51
II-6-2. Change the MeOperator's password (DCM server).....	52
II-6-3. Change the MeOperator's password (DCM add-on for SVS).....	53
II-6-4. Change the DcmOperator's password.....	54
III. Operation Checks	55
III-1. Operation Checks	56
III-1-1. Starting the DCM console	56
III-1-2. Uploading content.....	56
III-1-3. Schedule creation.....	58
III-1-4. Target registration.....	59
III-1-5. Update operation.....	62
III-1-6. Checking the update status	63
IV. Troubleshooting	65
IV-1. Network Checks.....	66
IV-1-1. Communication within the DCM system	66
IV-1-2. Checking the network communication	69
IV-2. Database Checks	70
IV-2-1. TCP/IP settings for SQL Server	70

IV-2-2. Settings for database connection	71
IV-3. FTP Server Checks	72
IV-3-1. Settings for FTP server connection	72
IV-4. Web Server Checks	73
IV-4-1. MIME settings (Windows Server 2008 R2)	73
IV-4-2. MIME settings (Windows Server 2008)	75
IV-5-3. MIME settings (Windows Server 2003 R2)	77
IV-5. NTP Server Settings	79
IV-5-1. NTP server settings	79
IV-5-2. NTP client settings	79
IV-6. Playback Client Settings	80
IV-6-1. Samba shared settings for storage type playback clients	80
IV-6-2. Set up ME-DEC, HDMA-4100 (if deliver contents via the Internet)	80
IV-7. Settings Required When Not Using a DNS Server	81
IV-7-1. Settings for MEDIAEDGE server	81
IV-8. Scheduled Serial Command Settings	82
IV-8-1. MEDIAEDGE server and STB Settings	82
IV-8-2. Storage type playback clients settings	83
IV-9. Ticker Content	84
IV-9-1. Encoding format for text files	84
IV-10. Log Files for MMSrv Service	85
IV-10-1. About log files for MMSrv service	85
IV-10-2. Messages related to the operation of the MMSrv service	86
IV-10-3. Messages related to SMIL file creation	86
IV-10-4. Messages related to download.txt file creation	87
IV-10-5. Messages related to download operations	92
IV-11. Log Files for MeRdSrv Service	95
IV-11-1. About log files for MeRdSrv service	95
IV-11-2. Messages related to the operation of the MeRdSrv service	96
IV-11-3. Messages related to the client	96
IV-11-4. Messages related to the schedule	97
IV-11-5. Messages related to the command schedule	98
IV-12. download.txt Files	99
IV-12-1. About download.txt files	99
IV-13. Windows Firewall Settings	101
IV-13-1. Firewall the installer set	101
The above firewall rules has been created during installation of DCM, though, unintentionally these rules might not work correctly. When such a case, please disable a firewall temporarily to check the operation. In this section, explains how to disable the firewall	101
IV-13-2. Windows Server 2008 R2	101
IV-13-3. Windows 7	102
IV-14. IIS Installation	103
IV-14-1. Windows Server 2008 R2	103
IV-14-2. Windows 7	107
IV-15. FTP Server Settings	108
IV-15-1. Windows Server 2008 R2	108
IV-15-2. Windows 7	112
IV-16. How to create a self-signed certificate	115

V. Appendix 117

V-1. Restrictions	118
V-1-1. DCM Installer specifications and restrictions	118
V-1-2. DCM console specifications and usage restrictions	118

- V-1-3. Usage restrictions for multiple DCM consoles 119
 - V-1-4. Region overlapping sequence 119
 - V-1-5. Availability of simultaneous playback..... 119
- V-2. How to start scheduled playback after restarting STB..... 120
 - V-2-1. Configuring the STB..... 120
 - V-2-2. Limitation as designed..... 120

Precautions for use

Regardless of whether or not there was negligence during use, we take no responsibility for indirect damages, including lost earnings, that arise from running this product, or for claims regarding such damages.

We make no guarantee whatsoever for the operation of the product for purposes other than those for which the product was designed, or in environments other than our recommended environments. Further, we make no guarantee whatsoever when this product is installed on a server computer or other computer that is used beyond its specifications, such as with an overclocked CPU.

Precautions regarding copyrighted material

Be aware of the following precautions when using this product to record the copyrighted material of third parties (examples: audio or video recorded on CDs, DVDs, video programs, etc., or acquired from radio or television broadcasts or Internet transmissions).

- Other than copying or editing for personal or household use, or for limited objectives based on these uses, copying or editing content may infringe the copyright. Before copying or editing can be performed, permission must be obtained from the copyright holder, via the right holder or right holder organization that is indicated on the storage media, or using another appropriate method.
- Copying or editing the copyrighted material of third parties and storing it on media for distribution or transmitting it via the Internet or any other method (including positing it on a website) is an infringement of the copyright, regardless of whether or not it was done for profit.
- Please understand in advance that we take no responsibility whatsoever for copyrighted materials or any copies that are created, copied or edited with this product.

Website

Please visit our web site to know support information or to get software updates.

<http://www.mediaedge-corp.com/>

I. Checks

This chapter describes the checks that should be performed before setup and the required precautions.

I-1. Overview of Display Content Manager

Display Content Manager (hereinafter referred to as "DCM") is special software for expanding the features of MEDIAEDGE4 (SVS4, STB4H, STB4, SWT4), HDMA-4100 and MEDIAEDGE Decoder (or ME-DEC), to make them compatible with digital signage (*1).

In video display systems that use Display Content Manager, playlists can be created to display multiple content items such as videos, still images and tickers on a single monitor, and scheduled playback of these playlists can then be performed.

*1: It also supports earlier products: MEDIAEDGE3 (SVS3, STB3 DS, SWT3 DS) and HDMA-4000/HDMA-4000 Sync.

- Flexible layout creation
 - Freely lay out multiple regions within the monitor (up to 20 regions).
 - You can adjust the size and position of the regions with intuitive mouse operations, or by entering numerical values.

- Wide variety of content types are available

Type of content	
Video	MPEG2 PS、MPEG2 TS、H.264
Audio	WAVE (PCM:8/16/24-bit, 1/2/5.1ch), MP3
Still images	BMP, JPEG, GIF (transparent GIF supported), PNG (transparent PNG supported)
Subtitles(Ticker)	TXT, XML (*2)
Flash	SWF (*3)
HTML	HTML
Quick Time	QuickTime (*4)
URI	URI to the above content
Control	ASCII string (HEX can also be specified) (*5)
Volume	Volume of playback clients (0 to 50 can be specified)

*2: RSS can be registered as URI content.

*3: STB and HDMA support Flash 7 or earlier versions. For SWT, Flash Player must be installed separately on the computer. ME-DEC is not support Flash content.

*4: QuickTime content is only supported for SWT4 local playback.

*5: Only sending is supported for control commands.

- Playlist creation
 - You can create a playlist by combining layouts and content.
 - You can perform preview playback of created playlists.
- Schedule creation
 - You can create a channel and set a schedule for delivering playlists.
- Playback client registration and schedule updating
 - You can link scheduled channels to playback clients to update the playback clients with schedules and content files.
 - You can set so that schedules and content files are updated regularly. You can also update by manual operation.
 - A differential update is performed when updating schedules and content files, so the data

I-2. Overview of the DCM Application

The DCM Application is comprised of three items, the DCM Console, the DCM Configuration Tool and the Status Monitor.

The main features of the DCM application are as follows.

- DCM Console
 - Content registration, uploading to the FTP server
 - Layout creation
 - Playlist creation
 - Schedule creation
 - Target (MEDIAEDGE server, playback clients) registration, automatic update setting, manual update operation
 - Status check when transferring data to the MEDIAEDGE server and playback clients
- DCM Configuration Tool
 - The Database settings
 - The DCM Console settings
- Status monitor
 - Playback status check for playback clients
 - Settings check for playback clients
 - Log collection for playback clients

The operating systems that support the installation of the DCM application are as follows.

- Windows Server 2012 (64bit) (Standard)
- Windows Server 2008 R2 (64bit) Service Pack 1 (Standard)
- Windows 8 (32bit / 64bit) (Pro / Enterprise)
- Windows 7 (32bit / 64bit) Service Pack1 (Professional / Enterprise / Ultimate)

The system requirements for the DCM application are as follows.

- CPU Intel Core 2 Duo 3 GHz or higher (*6)
- Memory 1 GB or higher
- Graphics Supports DirectX9, VRAM 256 MB or higher
- Screen resolution SVGA (800*600) or higher required; SXGA (1280*1024) or higher recommended (*7)
- Sound Onboard sound or sound card that supports stereo output
- Network 1000Base-T
- DVD-ROM drive Used for installation

*6: CPU must support the SSE2 instruction set. The DCM applications will not launch if the CPU does not support SSE2.

*7: Full HD (1920*1080) or WUXGA (1920*1200) is required for accurate preview playback.

About the installation location for the DCM application

If the DCM application is run on the DCM server or MEDIAEDGE server, the video distribution may become unstable. Use it temporarily for confirmation purposes only. We strongly recommend that you set up an operation PC that is separate from the server and that you use this operation PC for normal operations.

I-3. System Components

The DCM system is comprised of various devices that perform the roles described below, and the network that connects these devices. When constructing the DCM system, if you first confirm the roles that each device will perform, it will be easier to decide how to configure the system.

I-3-1. Operation PC

The operation PC is the computer on which the DCM application of Display Content Manager is installed. The DCM application is comprised of three items, the DCM Console, the DCM Configuration Tool and the Status Monitor. Almost all operations (*8) for system operation can be performed by using these three application items. At least one operation PC must be installed in the DCM system.

*8: When performing the initial settings and troubleshooting, the device settings must be checked and changed individually.

I-3-2. DCM server

The DCM server is the core feature of the DCM system and contains components such as the database. For this reason, only one (*9) DCM server must be installed in the DCM system.

*9: It is not possible to balance the access load distribution to the DCM server database or build redundancy. To prevent data loss in the event of hardware failure, be sure to perform independent backup of the database.

Database Management System (DBMS) is required for operating the DCM server. Display Content Manager supports the following DBMS.

- DBMS(*10)
 - SQL Server 2005
 - SQL Server 2008 R2
 - SQL Server 2012 (*11)

*10: SQL Server 2000, MSDE 2000 and earlier versions are not supported.

*11: Included with Display Content Manager Ver1.80.

The operating systems that support the installation of the DCM server are as follows.

- Windows Server 2012 (64bit) (Standard)
- Windows Server 2008 R2 (64bit) Service Pack 1 (Standard)
- Windows 8 (32bit / 64bit) (Pro / Enterprise)
- Windows 7 (32bit / 64bit) Service Pack1 (Professional / Enterprise / Ultimate)

The DCM server must be installed to the following if you want to distribute contents via the Internet.

- Windows Server 2012 (64bit) (Standard)
- Windows Server 2008 R2 (64bit) Service Pack 1 (Standard)

About the installation location for the DCM server

We recommend that a Windows Server operating system be used at the installation location of the DCM server. When a MEDIAEDGE server is used, it can be installed on the same server as the DCM server. Install on a Windows Client operating system (7, Vista, XP) only if a MEDIAEDGE server is not used and you cannot provide a separate Windows Server operating system for the DCM server.

For details on selecting the installation location, see [I-4 System Configuration].

I-3-3. FTP server

The FTP server is used as a relay point to which content files registered on the operation PC are uploaded, and from which the content files are then distributed to the MEDIAEDGE server or storage type playback clients. For this reason, at least one(*12) FTP server must be installed in the DCM system.

*12: Usually, only one is required. More can be added if required, for example, if there is insufficient storage capacity. Servers cannot be added for purposes such as balancing the access load distribution to the FTP server or for redundancy. To prevent data loss in the event of hardware

I-3-4. MEDIAEDGE-SVS server

The MEDIAEDGE-SVS server (selling separately) is a network video distribution server where MEDIAEDGE-SVS4 (or MEDIAEDGE-SVS3) software is installed. By installing [DCM add-on for SVS] onto the MEDIAEDGE-SVS server, you can add the feature to deliver contents from DCM system for digital signage. You can install or not install MEDIAEDGE server(s) in the DCM system.

The operating systems that support the installation of [DCM add-on for SVS] are as follows.

- MEDIAEDGE-SVS4
 - Windows Server 2012 (64bit) (Standard)
 - Windows Server 2008 R2 (64bit) Service Pack 1 (Standard)
 - Windows Server 2008 (32bit) Service Pack 2 (Standard)
 - Windows Server 2003 R2 (32bit) Service Pack 2 (Standard)

For details on the system requirements for the MEDIAEDGE-SVS server, see [MEDIAEDGESVS4 User's Guide] or [MEDIAEDGE-SVS3 User's Guide].

I-3-5. Playback clients

A playback client is a terminal that plays back a playlist that has been scheduled by the DCM console. At least one playback client must be installed in the DCM system. Playback clients can be broadly divided by their features into three categories.

STB

A Set Top Box (STB) is a hardware playback client that does not have internal storage, such as an HDD or SSD. It can play the video that is distributed by MEDIAEDGE-SVS server.

MEDIAEDGE-STB4H

MEDIAEDGE-STB4

MEDIAEDGE-STB3 DS (earlier product)



STB4H



STB4



STB3 DS

SWT

SWT is PC client software for using a PC as a playback client. A PC on which SWT is installed can play the video that is stored inside the internal storage inside the internal storage, or is distributed by MEDIAEDGE-SVS server. MEDIAEDGE-SVS is selling separately.

MEDIAEDGE-SWT4

MEDIAEDGE-SWT3 DS (earlier product)

ME-DEC, HDMA

ME-DEC or HDMA is a storage type of hardware playback client that uses an HDD or SSD as internal storage. It can play the video that is stored inside the internal storage, or is distributed by MEDIAEDGE server(*13).

ME-DEC (MEDIAEDGE Decoder)

HDMA-4100

HDMA-4000 (earlier product)

HDMA-4000 Sync (*14) (earlier product)



ME-DEC (MEDIAEDGE Decoder)



HDMA-4100



HDMA-4000



HDMA-4000Sync

*13: HDMA-4100 should be handled the same as STB4H. HDMA-4000 and HDMA-4000 Sync should be handled the same as STB3.

*14: The synchronization operation of HDMA-4000 Sync is not available with Display Content Manager. Register as HDMA-4000 when registering the client in the target window of the DCM console.

Playback clients can also be divided into two categories depending on how they are used: network type playback clients and storage type playback clients.

- **Network type playback client**
 - This is a network playback device that operates by receiving video streams from a MEDIAEDGE-SVS server.
 - ✧ STB
 - ✧ SWT
 - ✧ HDMA
- **Storage type playback client**
 - This is a stand-alone playback client that stores the content files and schedule files that are required for playback on its own internal storage.
 - ✧ SWT
 - ✧ HDMA
 - ✧ ME-DEC (MEDIAEDGE Decoder)

I-3-6. Network

The devices that comprise the DCM system (operation PC, FTP server, DCM server, MEDIAEDGE server, playback clients) must be connected in a network. Construct a local area network to enable communication between the devices.

Delivers contents via the Internet

DCM Ver.1.70 and later can deliver contents to ME-DEC or HDMA-4100 (Ver.2.0.0 or later) via the Internet without virtual local area network such as VPN. (Only when works as storage type playback client.)

I-4. System Configuration

To configure the DCM system, the devices that perform the various roles must be installed properly.

- Number of devices required for configuring the DCM system
 - Operation PC At least 1
 - FTP server Only 1 (*15)
 - DCM server Only 1 (*16)
 - MEDIAEDGE server 0 or more
 - Playback client At least 1

Examples of DCM system configurations are shown below.

*15: More can be added if required; for example, if there is insufficient storage capacity. Servers cannot be added for purposes such as balancing the access load distribution to the FTP server or for redundancy. As such, design a system configuration that has one server only.

*16: It is not possible to balance the access load distribution to the DCM server database or build redundancy. To prevent data loss in the event of hardware failure, be sure to perform independent backup of the database.

I-4-1. Smallest configuration without using a server

This is the smallest configuration, using one operation PC and storage type playback clients. The number of hardware units can be reduced by installing the FTP server and DCM server onto the same computer as the operation PC.

Before configuring this system, first consider whether to use the system configuration in [I-4-2 Configuration using a DCM server] or [I-4-3 Configuration using one MEDIAEDGE server].

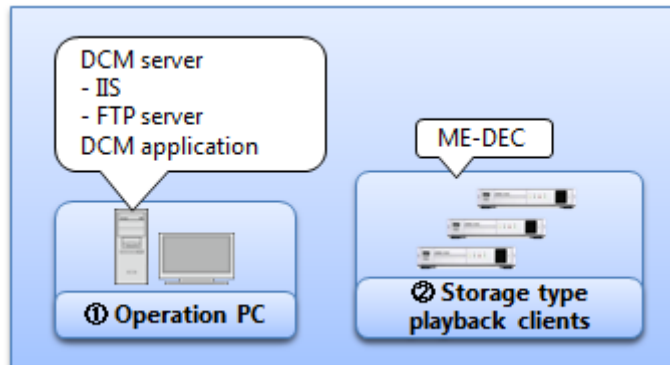


Fig. I-1 Configuration without using a server

(1) Operation PC (& FTP server, DCM server)

=> Set up the operation PC by following the steps below.

[1] [II-2-1 DCM server and DCM application installation]

(2) Storage type playback clients

=> Set up the storage type playback clients by following the steps below.

[1] IP address settings (*17)

[2] Operation mode settings (*18)

*17 : Please refer to the documentation of the Storage type playback clients.

*18 : ME-DEC : Setup boot mode to channel mode. HDMA : Setup boot mode to Schedule playback.

I-4-2. Configuration using a DCM server

This configuration uses one operation PC and one DCM server. The number of hardware units can be reduced by installing the FTP server onto the same server as the DCM server.

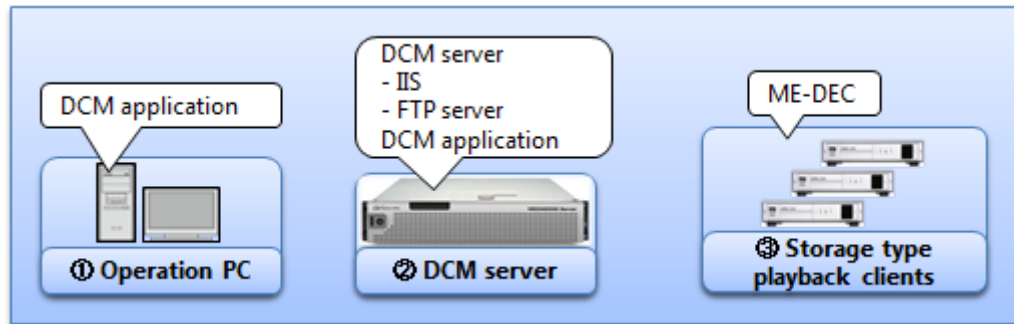


Fig. I-2 Configuration using a DCM server

(1) Operation PC

=> Set up the operation PC by following the steps below.

- [1] [II-2-2 DCM application installation]

(2) DCM server (& FTP server, operation PC)

=> Set up the DCM server by following the steps below.

- [1] [II-2-1 DCM server and DCM application installation]

(3) Storage type playback clients

=> Set up the storage type playback clients by following the steps below.

- [1] IP address settings (*19)
[2] Operation mode settings (*20)

*19 : Please refer to the documentation of the Storage type playback clients.

*20 : ME-DEC : Setup boot mode to channel mode. HDMA : Setup boot mode to Schedule playback.

I-4-3. Configuration using one MEDIAEDGE-SVS server

A configuration that uses one operation PC and one MEDIAEDGE-SVS server. (SVS is selling separately). The number of hardware units can be reduced by installing the FTP server and DCM server onto the same server as the MEDIAEDGE-SVS server.

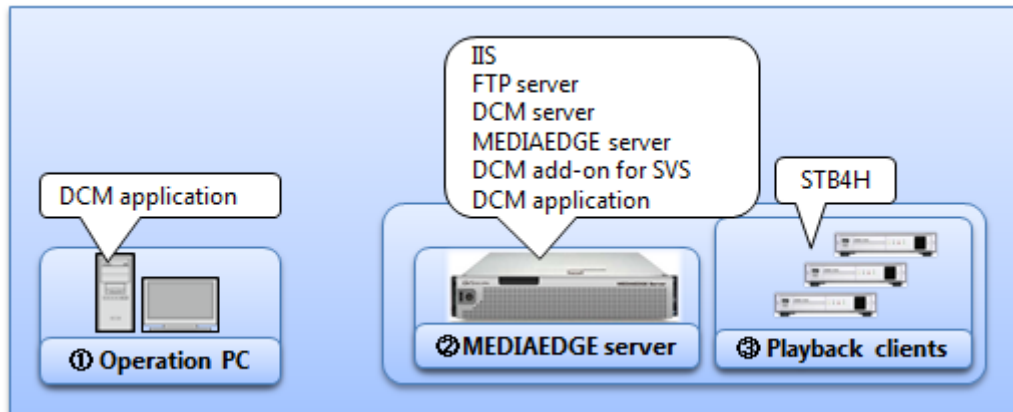


Fig. I-3 Configuration using a MEDIAEDGE server

(1) Operation PC

=> Set up the operation PC by following the steps below.

- [1] [II-2-2 DCM application installation]

(2) MEDIAEDGE server (& FTP server, DCM server, DCM add-on for SVS, operation PC)

=> Set up the MEDIAEDGE server by following the steps below.

- [1] [II-2-3 DCM server, DCM add-on for SVS and DCM application installation]
- [2] [II-4 MEDIAEDGE Server Installation]

(3) Network type playback clients

=> Set up the network type playback clients by following the steps below.

- [1] IP address settings (*21)
- [2] [V-2-1 Configuring the STB] (Channel mode settings)

*21: Please refer to the documentation of the network type playback clients.

I-4-4. Configuration using multiple MEDIAEDGE servers

A large-scale configuration that uses multiple operation PCs and multiple MEDIAEDGE servers. Also, a mixture of network type playback clients and storage type playback clients can be used as the playback clients. The number of hardware units can be reduced by installing the FTP server and DCM server onto one of the MEDIAEDGE servers.

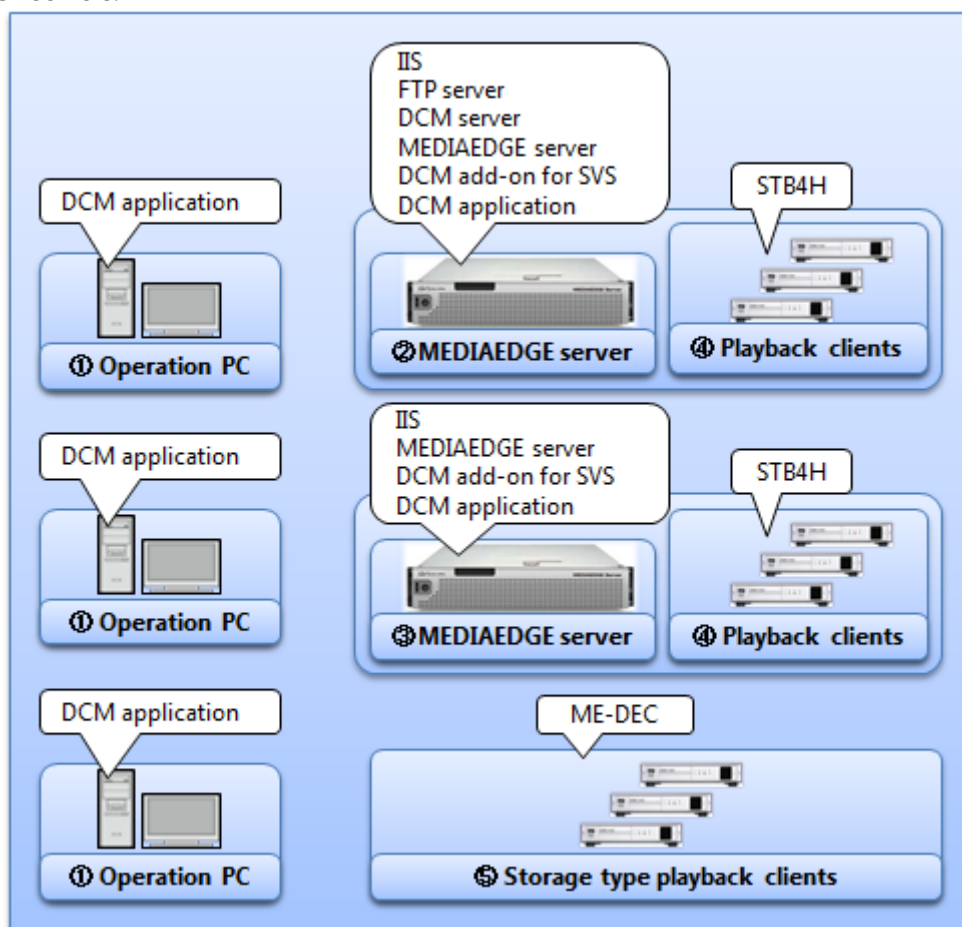


Fig. I-4 Configuration using multiple MEDIAEDGE servers

(1) Operation PC

=> Set up the operation PC by following the steps below.

[1] [II-2-2 DCM application installation]

(2) MEDIAEDGE server (& FTP server, DCM server, DCM add-on for SVS, operation PC)

=> Set up the MEDIAEDGE server by following the steps below.

[1] [II-2-3 DCM server, DCM add-on for SVS and DCM application installation]

[2] [II-4 MEDIAEDGE Server Installation]

(3) MEDIAEDGE server (& DCM add-on for SVS, operation PC)

=> Set up the MEDIAEDGE server by following the steps below.

[1] [II-2-3 DCM server, DCM add-on for SVS and DCM application installation] (*22)

[2] [II-4 MEDIAEDGE Server Installation]

[*22: Please deselect the DCM Server at feature selection screen during installation..](#)

(4) Network type playback clients

=> Set up the network type playback clients by following the steps below.

[1] IP address settings (*23)

[2] [V-2-1 Configuring the STB] (Channel mode settings)

[*23: Please refer to the documentation of the network type playback clients.](#)

(5) Storage type playback clients

=> Set up the storage type playback clients by following the steps below.

[1] IP address settings (*24)

[2] Operation mode settings (*25)

[*24 : Please refer to the documentation of the Storage type playback clients.](#)

[*25 : ME-DEC : Setup boot mode to channel mode. HDMA : Setup boot mode to Schedule playback.](#)

I-4-5. Large-scale configuration that separates all server functions

A large-scale configuration that uses multiple operation PCs and multiple MEDIAEDGE servers. Also, a mixture of network type playback clients and storage type playback clients can be used as the playback clients. In this configuration, both the FTP server and DCM server are installed on hardware units that are separate from the MEDIAEDGE server.

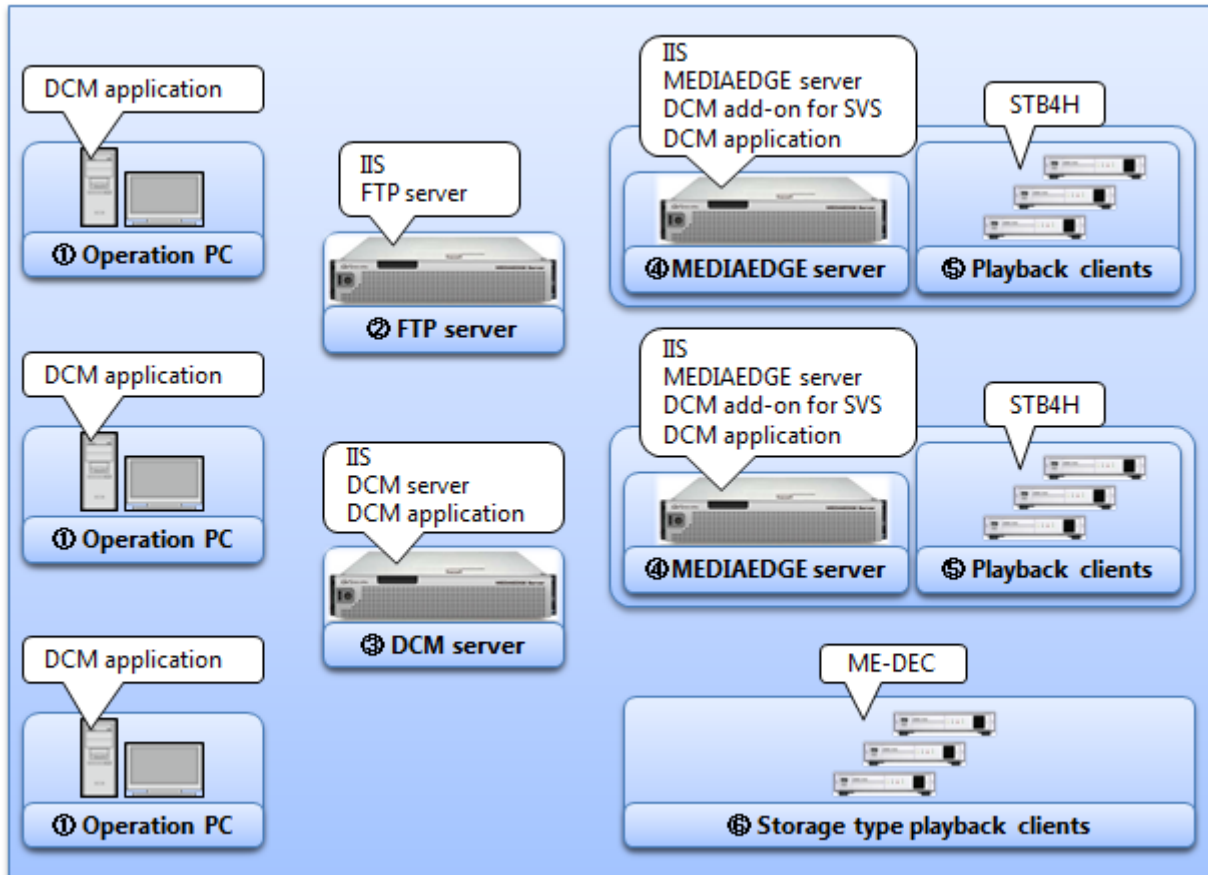


Fig. I-5 Large-scale configuration

(1) Operation PC

=> Set up the operation PC by following the steps below.

[1] [II-2-2 DCM application installation]

(2) FTP server

=> Set up the FTP server by following the steps below.

[1] [IV-15. FTP Server Settings]

(3) DCM server (& operation PC)

=> Set up the DCM server by following the steps below.

[1] [II-2-1 DCM server and DCM application installation]

(4) MEDIAEDGE server (& DCM add-on for SVS, operation PC)

=> Set up the MEDIAEDGE server by following the steps below.

[1] [II-2-3 DCM server, DCM add-on for SVS and DCM application installation] (*26)

[2] [II-4 MEDIAEDGE Server Installation]

[*26: Please deselect the DCM Server at feature selection screen during installation.](#)

(5) Network type playback clients

=> Set up the network type playback clients by following the steps below.

[1] IP address settings (*27)

[2] [V-2-1 Configuring the STB] (Channel mode settings)

[*27: Please refer to the documentation of the network type playback clients.](#)

(6) Storage type playback clients

=> Set up the storage type playback clients by following the steps below.

[1] IP address settings (*28)

[2] Operation mode settings (*29)

[*28 : Please refer to the documentation of the Storage type playback clients.](#)

[*29 : ME-DEC : Setup boot mode to channel mode. HDMA : Setup boot mode to Schedule playback.](#)

I-4-6. Configuration that delivers contents via the Internet

A configuration that delivers contents from one or more operation PCs to playback clients which are deployed in wide area via the DCM server and the FTP server which are located in the Internet. This configuration will be possible only if the ME-DEC or HDMA-4100 (version 2.0.0 and later) is acting as a storage type playback client. In addition, you will need to install the DCM server on the following OS.

- * Windows Server 2012 (64bit) (Standard)
- * Windows Server 2008 R2 (64bit) SP1 (Standard)

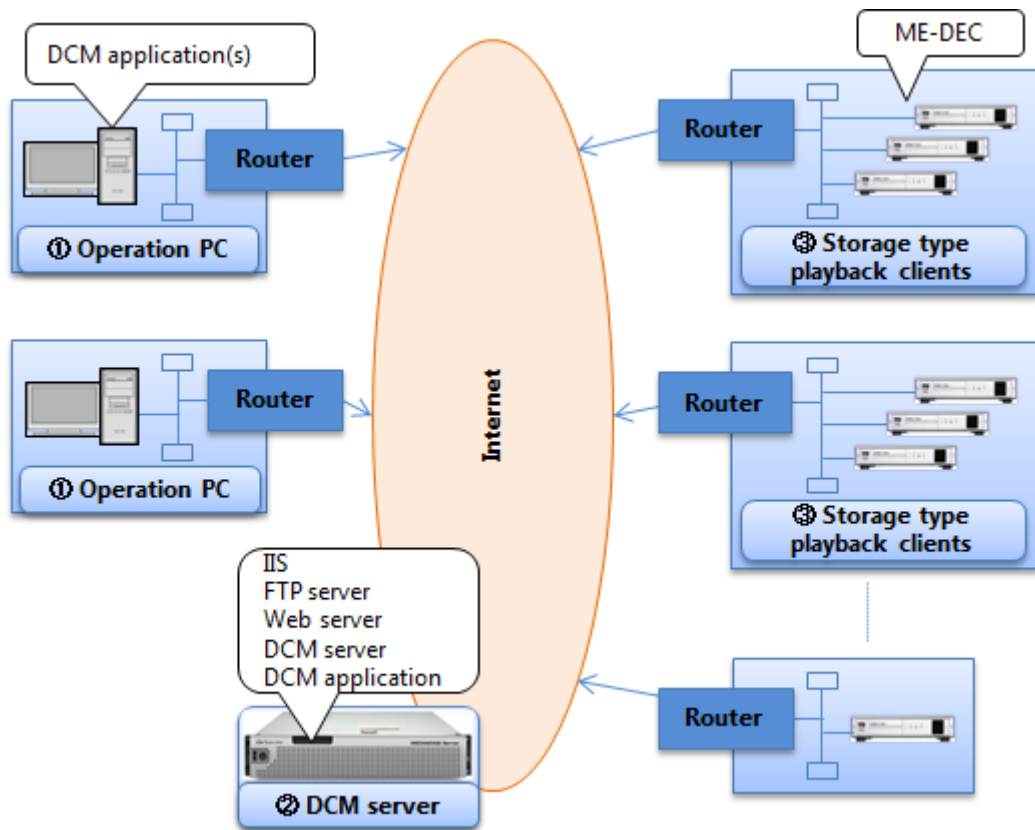


Fig. I-6 Configuration that delivers contents via the Internet

(1) Operation PC (*30)

=> Set up the operation PC by following the steps below.

[1] [II-2-2 DCM application installation]

*30 : Must be able to access the DCM server which is located in the Internet from the operation PC.

(2) DCM server (& FTP server, Web server, operation PC) (*31)

=> Set up the DCM server by following the steps below.

[1] [II-2-1 DCM server and DCM application installation] (*32)

*31 : DCM server must be located in the Internet.

*32 : Windows firewall, FTP server, Web server will be set up by the DCM installer.

(3) Storage type playback clients (*33)

=> Set up the storage type playback clients by following the steps below.

[1] IP address settings (*34)

[2] Operation mode settings (*35)

[3] [IV-6-2. Set up ME-DEC, HDMA-4100 (if deliver contents via the Internet)]

*33 : Must be able to access the DCM server which is located at the Internet from the storage type playback clients.

*34 : Please refer to the documentation of the Storage type playback clients.

*35 : ME-DEC : Setup boot mode to channel mode. HDMA : Setup boot mode to Schedule playback.

II. Setup

This chapter describes the various setup methods.

II-1. Network Settings

Unless otherwise noted, this chapter uses the following network settings as the basis for its explanations.

Operation PC

- Computer name OperationPC
- IP address 192.168.1.10
- Subnet mask 255.255.255.0
- Default gateway 192.168.1.254
- Preferred DNS server 192.168.1.1
- Alternate DNS server (None)

FTP server

- Computer name FTP-SVR
- IP address 192.168.1.20
- Subnet mask 255.255.255.0
- Default gateway 192.168.1.254
- Preferred DNS server 192.168.1.1
- Alternate DNS server (None)

DCM server

- Computer name DCM-SVR
- IP address 192.168.1.30
- Subnet mask 255.255.255.0
- Default gateway 192.168.1.254
- Preferred DNS server 192.168.1.1
- Alternate DNS server (None)

MEDIAEDGE server

- Computer name MEDIAEDGE-SVR
- IP address 192.168.1.1
- Subnet mask 255.255.255.0
- Default gateway 192.168.1.254
- Preferred DNS server 192.168.1.1
- Alternate DNS server (None)

Network type playback clients, Storage type playback clients

- IP address Range from 192.168.1.101 to 192.168.1.200
- Subnet mask 255.255.255.0
- Default gateway 192.168.1.254
- Preferred DNS server 192.168.1.1
- Alternate DNS server (None)

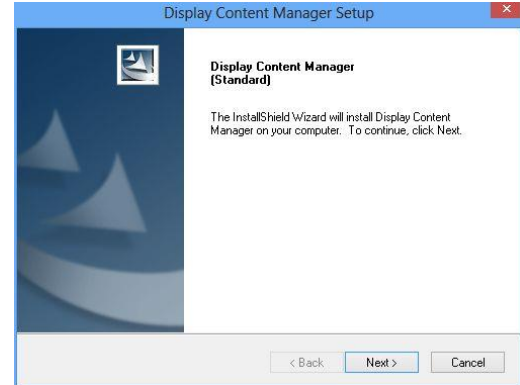
II-2. Display Content Manager Installation

This section describes the procedure for installing Display Content Manager.

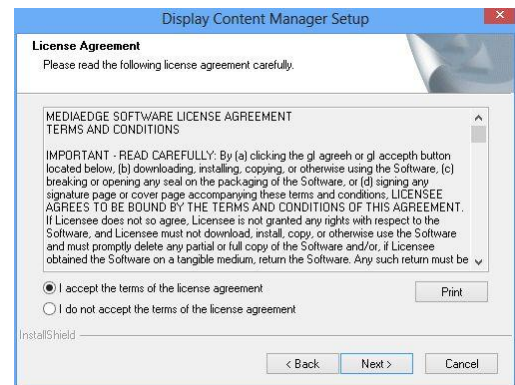
II-2-1. DCM server and DCM application installation

This section describes the procedure for installing the DCM server and DCM application.

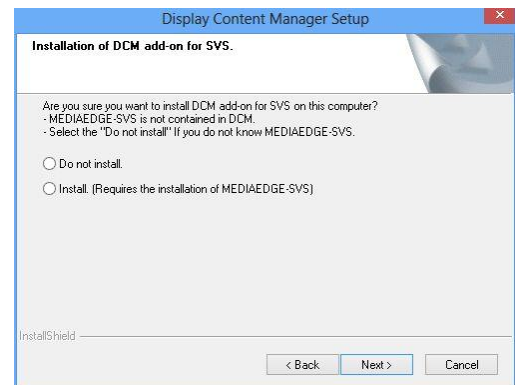
1. Insert the [Display Content Manager Installation Disc] into the DVD-ROM drive.
2. In the DVD-ROM drive, open the [DCM] folder and double-click [Setup.exe].
3. Click [Next].



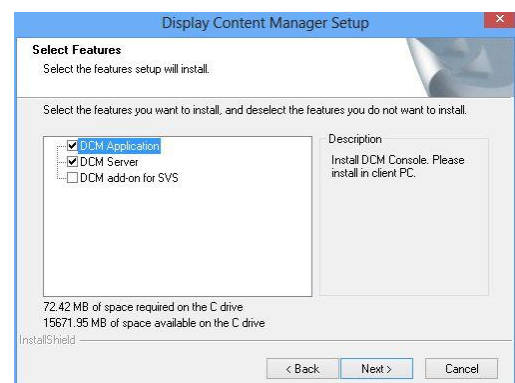
4. Select [I accept the terms of the license greement], and click [Next].



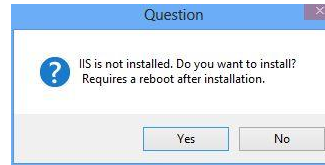
5. Select [Do not install] and click [Next].



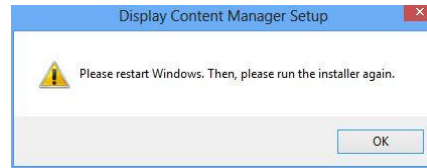
6. Select [DCM Application] and [DCM Server]



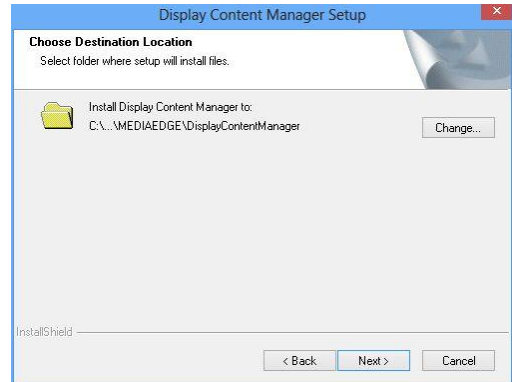
7. Click [Yes].
Install IIS, DotNet Framework 4.5 is started. It takes about 5 minutes.



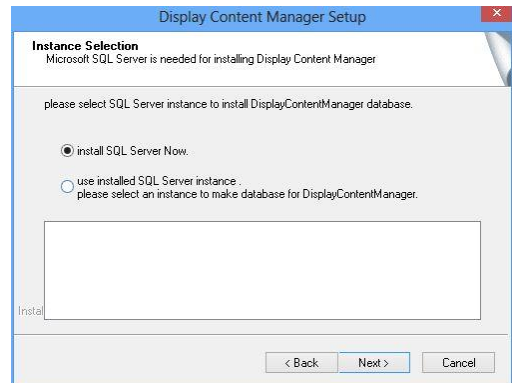
8. Click [OK]. Then, please **restart** the OS.
After restarting, follow the procedure [1]-[6] again, and then go to the procedure



9. Click [Next].
To change the installation location, click [Change] and select an installation location.

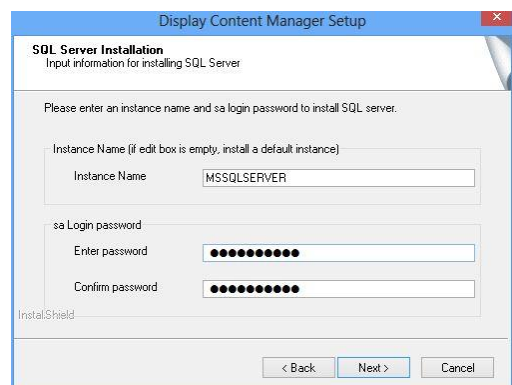


10. Select [install SQL Server Now] and click [Next].
If SQL Server is already installed, select [use installed SQL Server instance], select an installed instance, and click [Next].

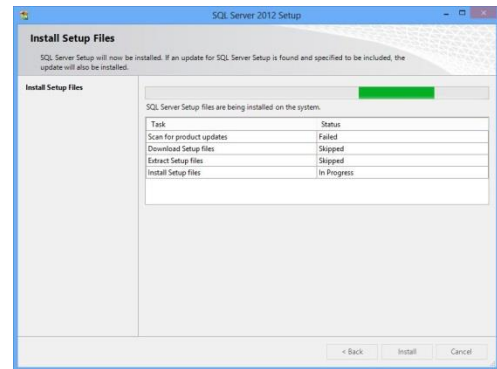


11. Enter [sa Login password], and then click [Next].
=> The installation of SQL Server starts.
We recommend leaving the instance name blank. When the

Default Instance=MSSQLSERVER
Default Password=Mediaedge4

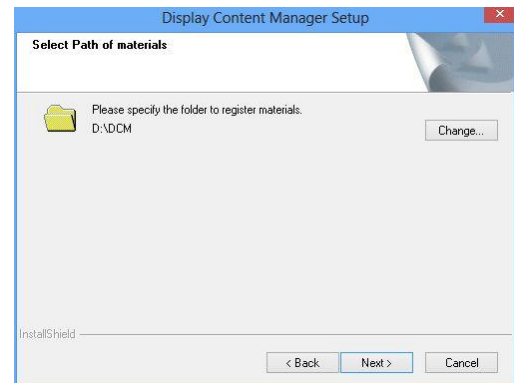


12. It takes about 10 minutes.



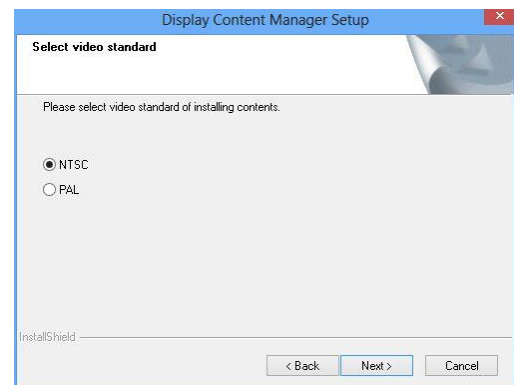
13. Select the path that preserves content files, and then click [Next].

Because the content files that are registered with the DCM console are stored in this folder, specify a drive that has a lot of free space.

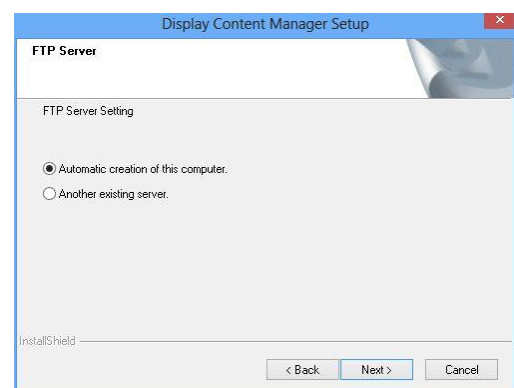


14. Select the broadcast standard for the sample contents, and then click [Next].

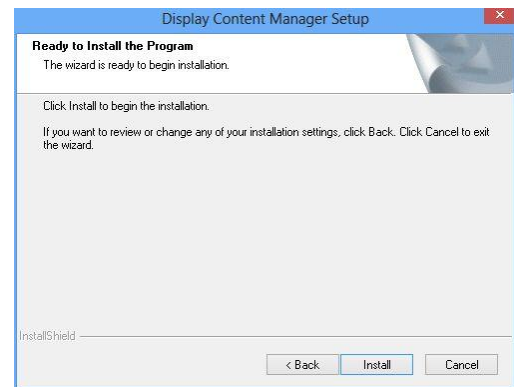
Select the broadcast standard that is used in your region (NTSC or PAL).



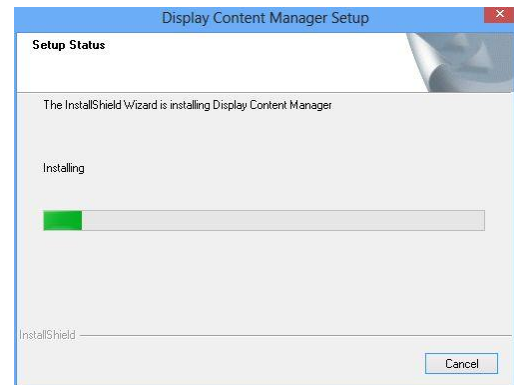
15. Select [Automatic creation of this computer.] and click [Next].



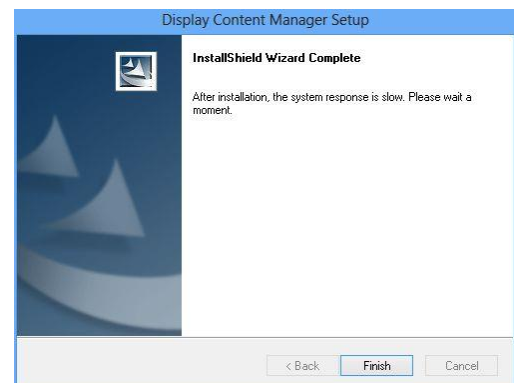
16. Click [Install].
=> The installation starts.



17. It takes about 10 minutes.



18. This completes the installation.
There are cases where the response of the system slows down immediately after installation. Please wait.

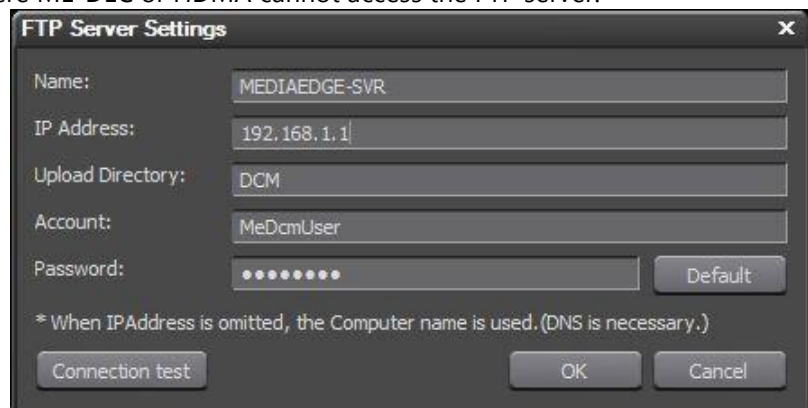


For the IP address of the FTP server

If the computer name is not DNS registration, you need to set the IP address.

The DCM console [Options] - [FTP server], please set the IP address.

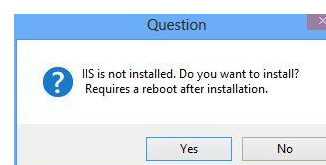
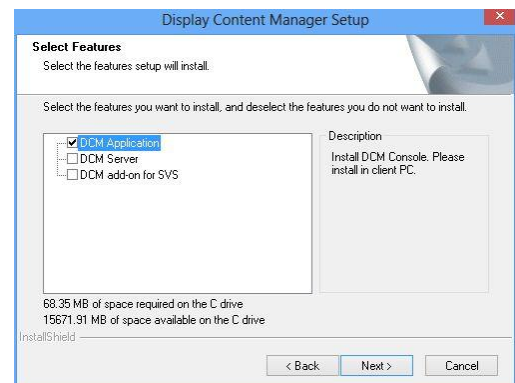
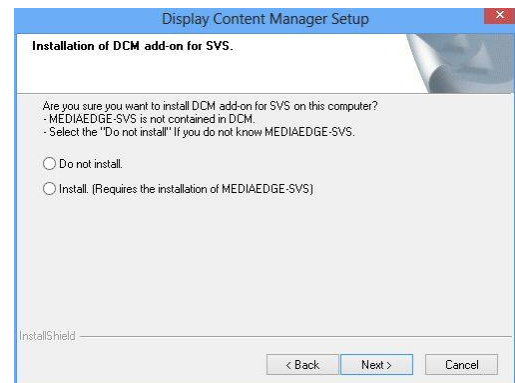
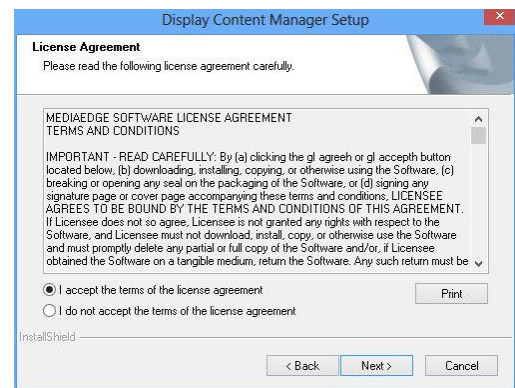
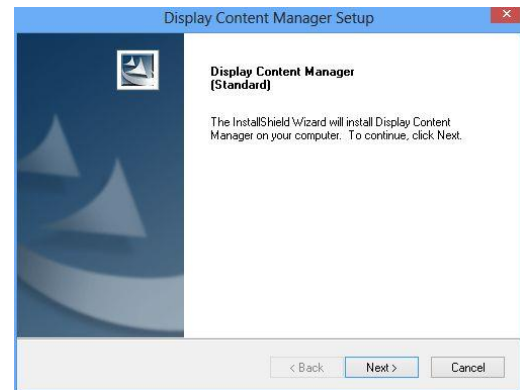
There are cases where ME-DEC or HDMA cannot access the FTP server.



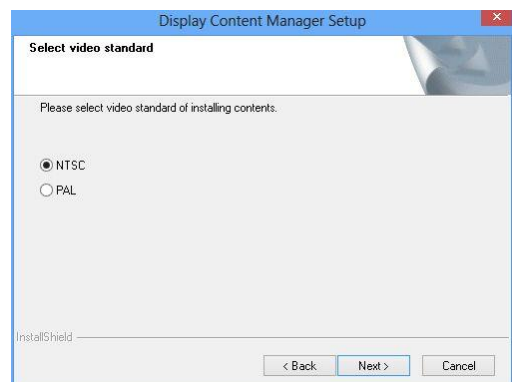
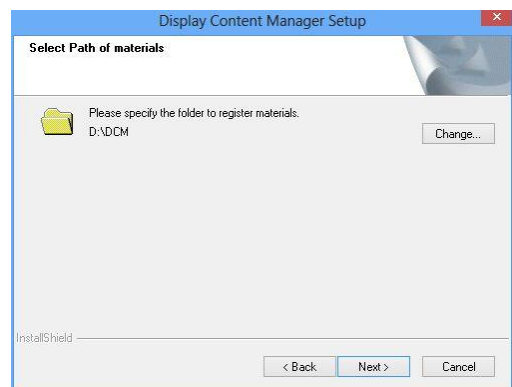
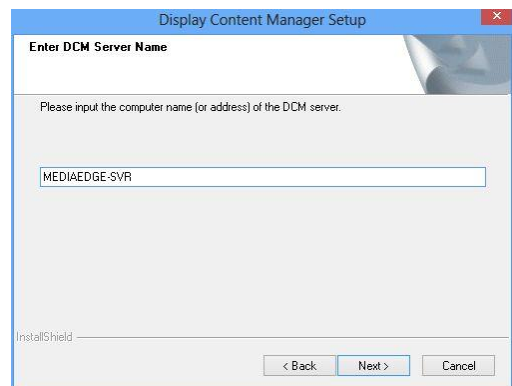
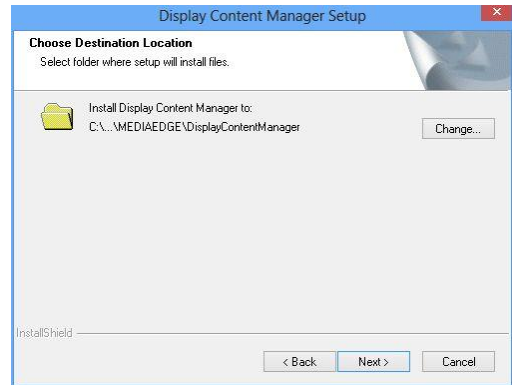
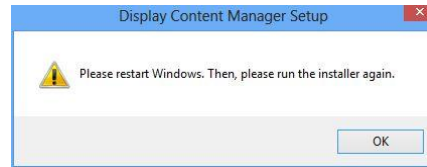
II-2-2. DCM application installation

This section describes the procedure for installing the DCM application.

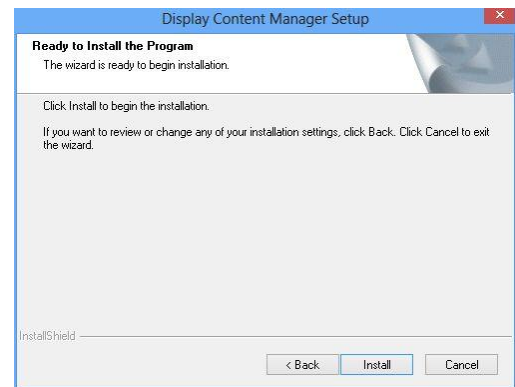
1. Insert the [Display Content Manager Installation Disc] into the DVD-ROM drive.
2. In the DVD-ROM drive, open the [DCM] folder and double-click [Setup.exe].
3. Click [Next].
4. Select [I accept the terms of the license greement], and click [Next].
5. Select [Do not install] and click [Next].
6. Select [DCM Application]
7. Click [Yes].
Install IIS, DotNet Framework 4.5 is started. It takes about 5 minutes.



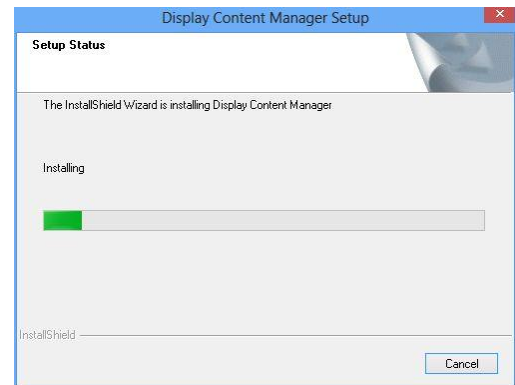
8. Click [OK]. Then, please **restart** the OS.
After restarting, follow the procedure [1]-[6] again, and then go to the procedure
9. Click [Next].
To change the installation location, click [Change] and select an installation location.
10. Enter the name of the DCM server computer, and then click [Next].
In a network environment that does not have a DNS server and cannot perform name resolution, enter the IP address of the DCM server.
11. Select the path that preserves content files, and then click [Next].
Because the content files that are registered with the DCM console are stored in this folder, specify a drive that has a lot of free space.
12. Select the broadcast standard for the sample contents, and then click [Next].
Select the broadcast standard that is used in your region (NTSC or PAL).



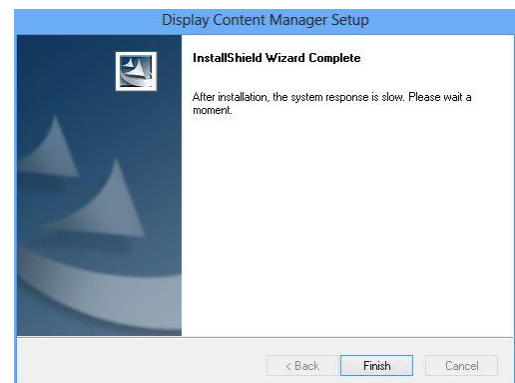
13. Click [Install].
=> The installation starts.



14. It takes about 10 minutes.



15. This completes the installation.
There are cases where the response of the system slows down immediately after installation. Please wait.

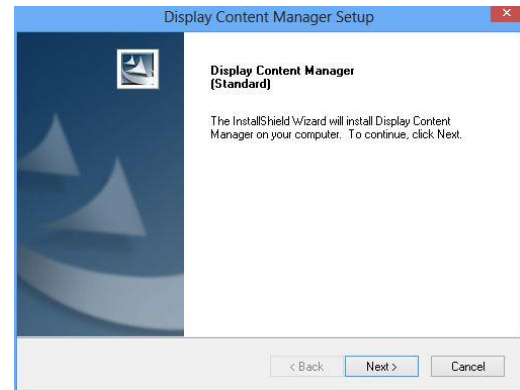


II-2-3. DCM server, DCM add-on for SVS and DCM application installation

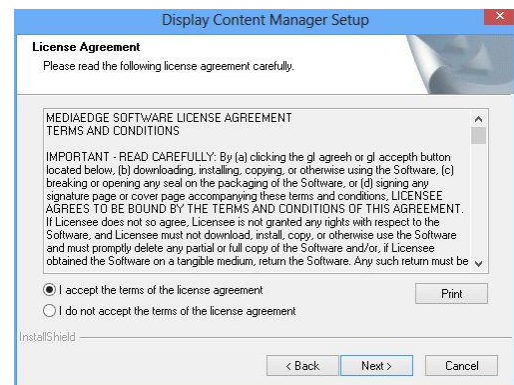
This section describes the procedure for installing Display Content Manager.

*MEDIAEDGE-SVS must be installed separately later.

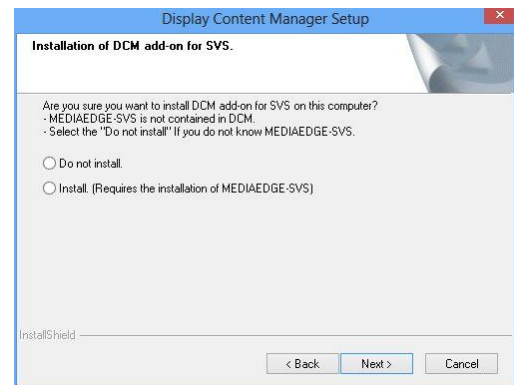
1. Insert the [Display Content Manager Installation Disc] into the DVD-ROM drive.
2. In the DVD-ROM drive, open the [DCM] folder and double-click [Setup.exe].
3. Click [Next].



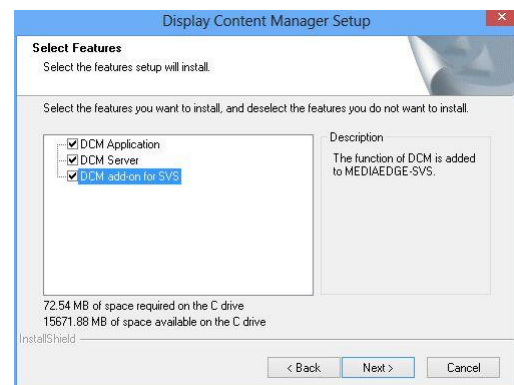
4. Select [I accept the terms of the license greement], and click [Next].



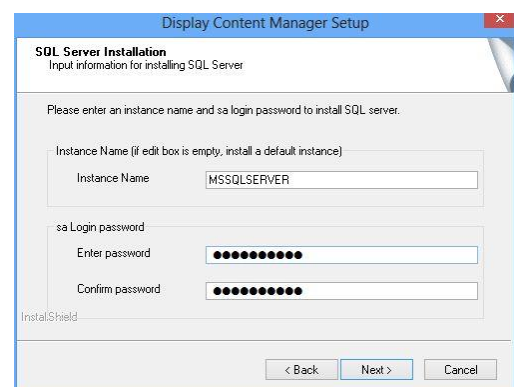
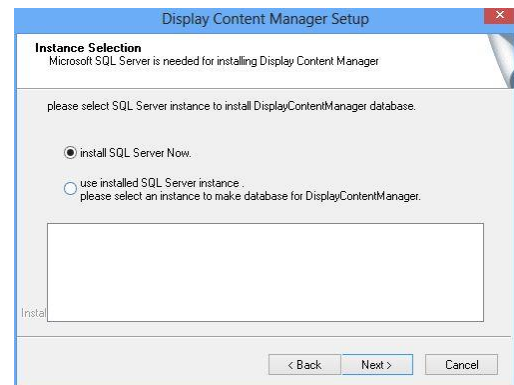
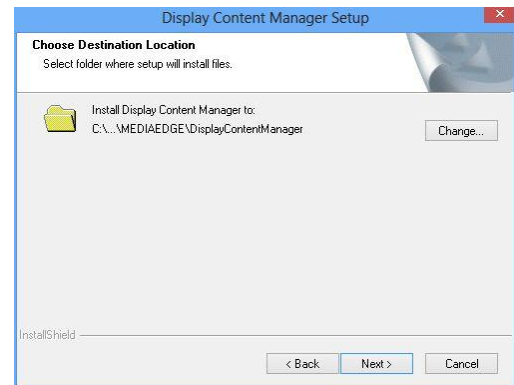
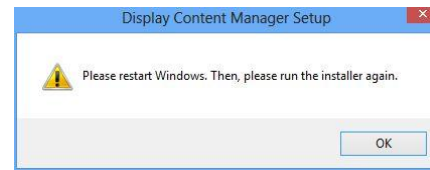
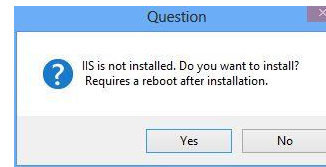
5. Select [install] and click [Next].



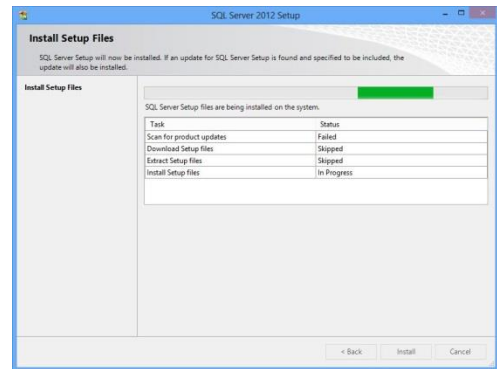
6. Select [DCM Application] and [DCM Server] and [DCM add-on for SVS]
If you had already installed DCM server onto another server in your DCM system, please deselect [DCM Server].



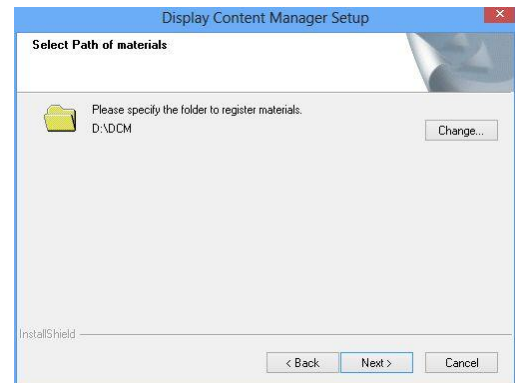
7. Click [Yes].
Install IIS, DotNet Framework 4.5 is started. It takes about 5 minutes.
8. Click [OK]. Then, please **restart** the OS.
After restarting, follow the procedure [1]-[6] again, and then go to the procedure
9. Click [Next].
To change the installation location, click [Change] and select an installation location.
10. Select [install SQL Server Now] and click [Next].
If SQL Server is already installed, select [use installed SQL Server instance], select an installed instance, and click [Next].
11. Enter [sa Login password], and then click [Next].
=> The installation of SQL Server starts.
We recommend leaving the instance name blank. When the
Default Instance=MSSQLSERVER
Default Password=Mediaedge4



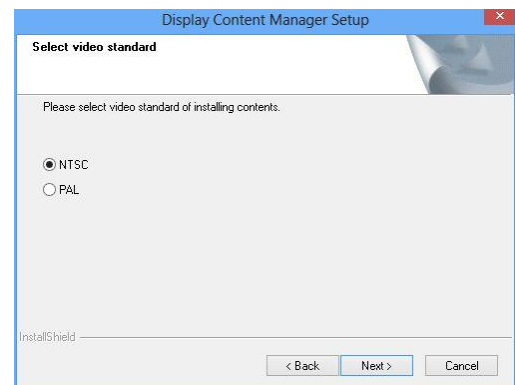
12. It takes about 10 minutes.



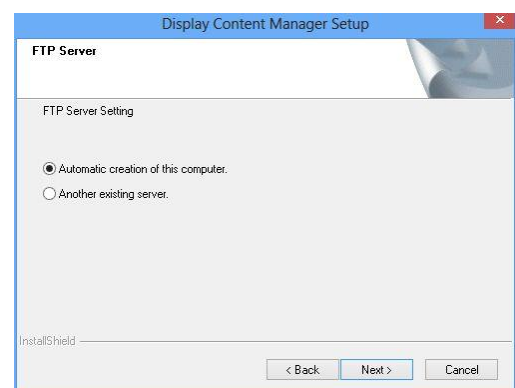
13. Select the path that preserves content files, and then click [Next].
 # Because the content files that are registered with the DCM console are stored in this folder, specify a drive that has a lot of free space.



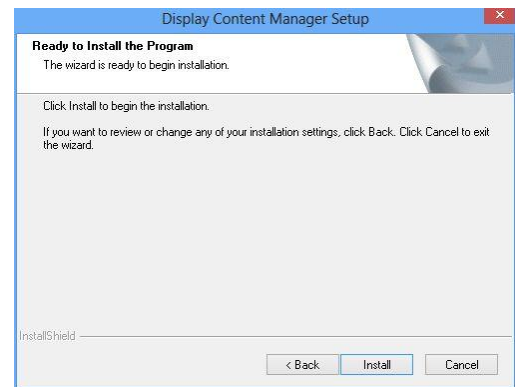
14. Select the broadcast standard for the sample contents, and then click [Next].
 # Select the broadcast standard that is used in your region (NTSC or PAL).



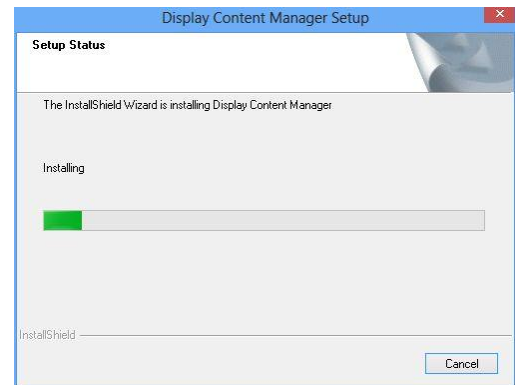
15. Select [Automatic creation of this computer.] and click [Next].



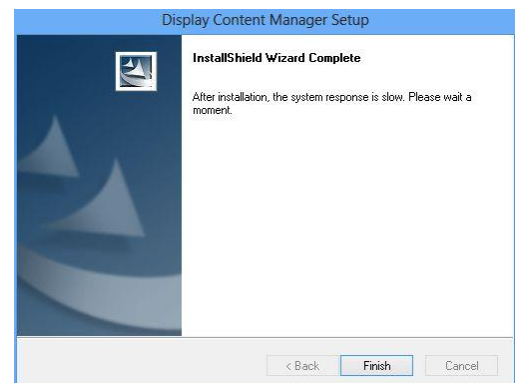
16. Click [Install].
=> The installation starts.



17. It takes about 10 minutes.



18. This completes the installation.
There are cases where the response of the system slows down immediately after installation. Please wait.



II-3. DCM Config Tool

II-3-1. DataBase Connection

The screenshot shows the 'DCM configuration tool' window with the 'Step1 DataBase Connection' tab selected. The 'DataBase' section contains input fields for 'Computer name' (localhost), 'Instance name' (empty), and 'Port number' (1433). The 'Authentication' section has radio buttons for 'Windows' and 'SQL' (selected), with corresponding 'Username' (DcmOperator) and 'Password' (masked) fields. An 'Initialize' button is next to the password field. Below this is a 'Connection Successful' status area with a 'Connection test' button. The 'Products used' section lists several products with checkboxes: HDMA-4000, HDMA-4100, DEC (checked), STB3, STB4, STB4H, SWT3-DS, SWT4 (checked), and HDSS-4Km1 (checked). At the bottom, the 'Material path' is set to 'D:\DCM', and a 'Next after setting' button is located in the bottom right corner.

Name	Default	Description
Computer name	"Computer name"	DCM Server's computer name or an IP address. When an own computer is a DCM server, you can specify "localhost".
Instance name	"Blank"	The instance name of SQL Server
Port number	1433	The port number of SQL Server
Authentication	SQL	Windows --- uses a Windows user. SQL --- uses a SQL Server user.
Username	DcmOperator	Used when authentication is SQL.
Password	*****	Used when authentication is SQL.
Products used	ME-DEC, SWT4, HDSS-4K	Select products which appear in the choice when new playlist and such will be created. If you want to use ME-DEC only, please check only ME-DEC.

II-3-2. Server Conenction

The screenshot shows the 'DCM configuration tool' window with three tabs: 'Step1 DataBase Connection', 'Step2 Server Connection' (active), and 'Step3 Others'. The 'DCM server' section contains the following fields and buttons:

- Server name: User-PC
- IP address: (empty)
- Username: MeOperator
- Password: (masked with dots)
- Initialize button
- Timeout: 60 Second
- Connection Successful(HTTPS) status
- Connection test button

The 'File server' section has a checkbox for 'Use HTTP/HTTPS to download' which is currently unchecked.

The 'Proxy' section includes the following fields:

- All Proxy Host: (empty)
- HTTP Proxy Host: (empty)
- All Proxy Port: 0
- HTTP Proxy Port: 0
- NoProxy: (empty)
- FTP Proxy Host: (empty)
- FTP Proxy Port: 0

At the bottom, there are 'Back' and 'Next after setting' buttons.

Name	Default	Description
Server name	"Computer name"	Computer name of the DCM server
IP address	"blank" or "IP address"	IP address of the DCM server. (It uses the server name if omitted)
Username	MeOperator	This user is set by the installer.
Password	*****	This user is set by the installer.
Timeout	60 (sec)	Specify a time-out value when "Get Status" operation has executed in DCM Console.
File Server	No check	Check to use HTTP (or HTTPS), not FTP when delivering the materials. HDMA-4000 and old version of HDMA-4100 cannot download using HTTP.
Proxy	Host="blank" Port=0	In case of blank (= not use), [Control Panel] - [Internet Options] will be used.

II-4. MEDIAEDGE-SVS Server Installation

II-4-1. SVS4 installation

This section describes the procedure for installing MEDIAEDGE-SVS4. MEDIAEDGE-SVS is selling separately.

About the network settings for the MEDIAEDGE server

For details on the individual settings for the MEDIAEDGE server, see the sections such as [Chapter 2 1-3. About the settings during OS installation] and [Chapter 2 3. Connecting to clients] in [MEDIAEDGE-SVS4 User's Guide].

About dongle connection

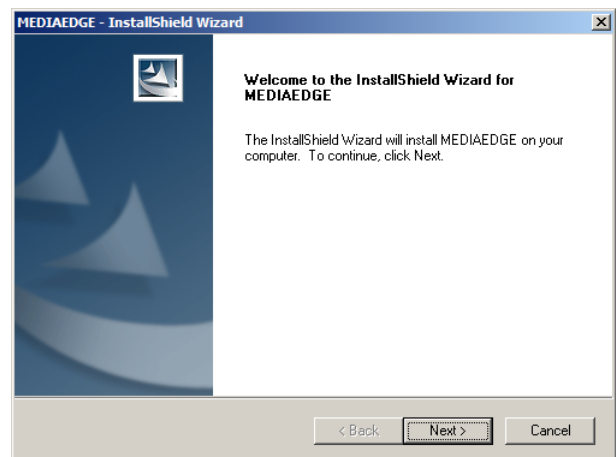
If you connect the dongle before performing the installation, the dongle may not be recognized. Connect the dongle when the prompt message appears during the dongle driver installation.

About the installation sequence for SVS4 and SQL Server 2005 Express Edition

Although in [MEDIAEDGE-SVS4 User's Guide], [Chapter 2 1-4. DBMS installation] is performed before [Chapter 2 2. SVS4 installation], we recommend you use DBMS which has been already installed, as described in this section.

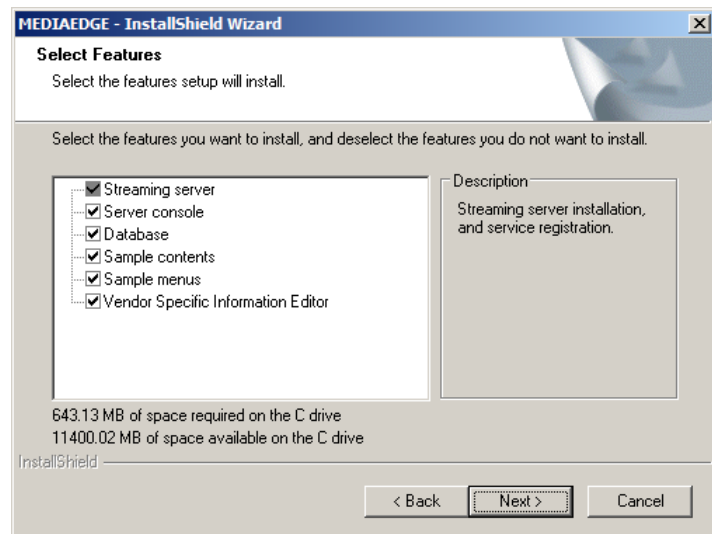
If DBMS has been installed separately, the TCP/IP protocol is disabled. Change the setting by following the steps in p.194 [IV-2 Database Checks].

- [1] Insert the [MEDIAEDGE-SVS4 Installation DVD] into the DVD-ROM drive.
- [2] In the DVD-ROM drive, open the [SVS] folder and double-click [Setup.exe].
- [3] Click [Next].



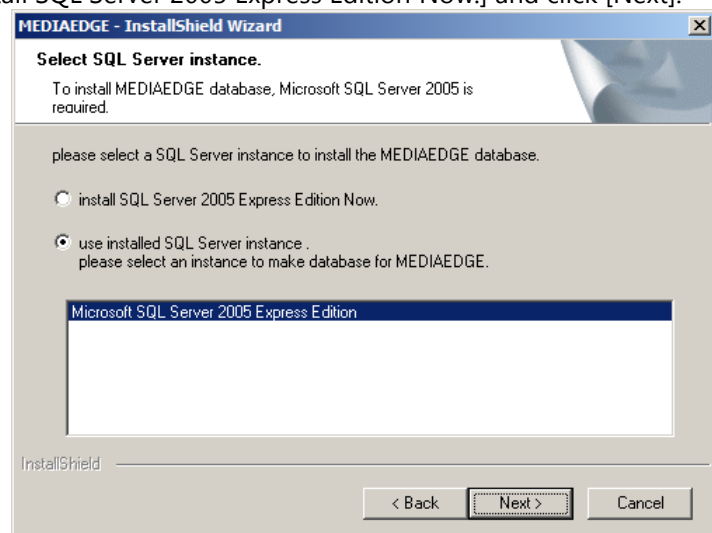
[4] Select the components to install and click [Next].

Unless you are dividing the components for installation on multiple computers, keep all the check boxes selected and click [Next].



[5] Select [use installed SQL Server instance.], select an installed instance, and click [Next].

If there is no installed instance, select [install SQL Server 2005 Express Edition Now.] and click [Next].



If you selected [install SQL Server 2005 Express Edition Now.].

Enter [sa Login password], and then click [Next]. The installation of SQL Server 2005 Express Edition starts.

We recommend leaving the instance name blank. When the field is blank, the default instance is installed.

Enter any password for the system administrator (sa) login password. (*1)

Keep a record of the system administrator (sa) login password in a safe place to make sure you do not forget it.

The screenshot shows the 'MEDIAEDGE - InstallShield Wizard' window. The title bar is blue with the text 'MEDIAEDGE - InstallShield Wizard' and a close button. The main content area has a light gray background. At the top, it says 'SQL Server Installation' and 'Input information for installing SQL Server 2005 Express Edition'. Below this, it says 'Please enter an instance name and sa login password to install SQL server.' There are two main sections: 'Instance Name (if edit box is empty, install a default instance)' with a text box labeled 'Instance Name' that is currently empty, and 'sa Login password' with two text boxes labeled 'Enter password' and 'Confirm password', both containing masked characters (dots). At the bottom right, there are three buttons: '< Back', 'Next >' (which is highlighted with a dashed border), and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner of the dialog box.

*1 : In environments where blank passwords are not allowed, enter a password that conforms to the password policy.

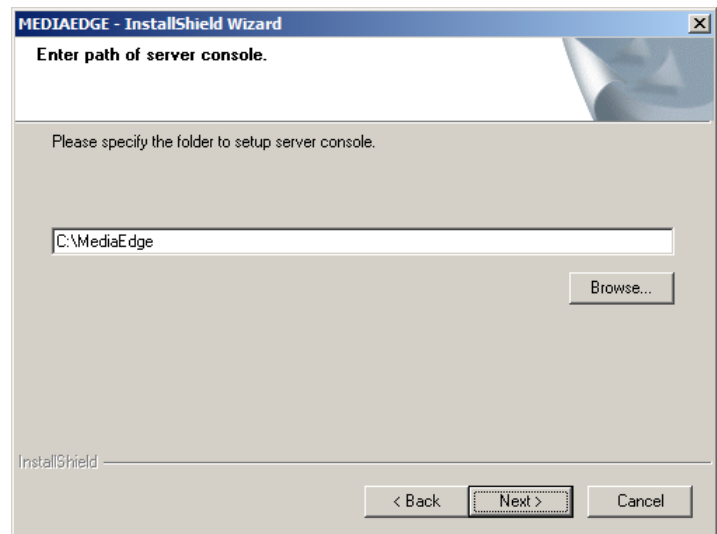
[6] Enter the name of the database to use on the MEDIAEDGE server, and then click [Next].

Usually, use the default, [MEDIAEDGE_DB].

The screenshot shows the 'MEDIAEDGE - InstallShield Wizard' window. The title bar is blue with the text 'MEDIAEDGE - InstallShield Wizard' and a close button. The main content area has a light gray background. At the top, it says 'Enter MEDIAEDGE database name.' Below this, it says 'Please set the database name. '' is not allowed.' There is a single text box containing the text 'MEDIAEDGE_DB'. At the bottom right, there are three buttons: '< Back', 'Next >' (which is highlighted with a dashed border), and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner of the dialog box.

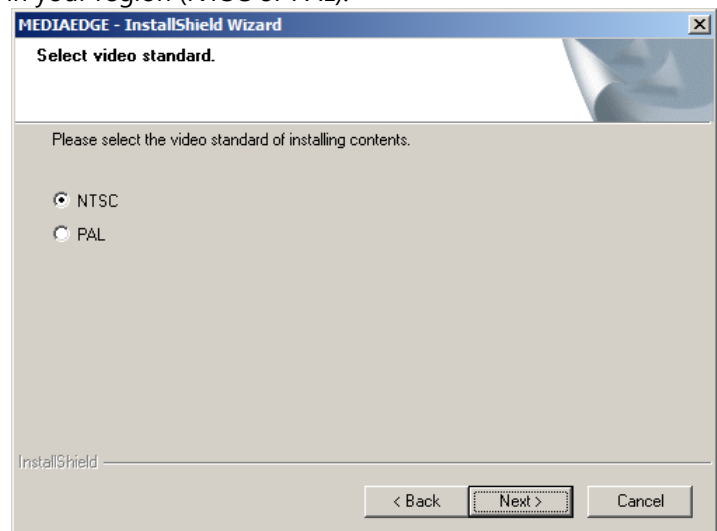
[7] Set the folder for setting up the server console, and then click [Next].

The folder that you specify here will store the server console and the webpage files for the sample menus.



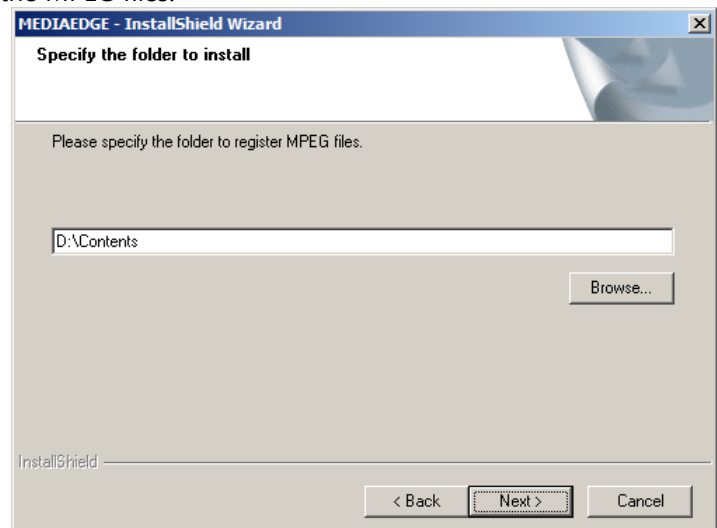
[8] Select the broadcast standard for the content, and then click [Next].

Select the broadcast standard that is used in your region (NTSC or PAL).



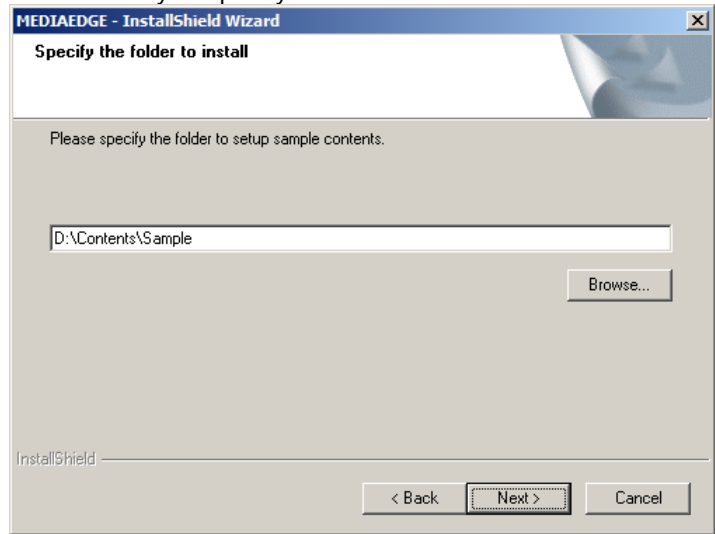
[9] Set the folder for registering MPEG files, and then click [Next].

The folder that you specify here will store the MPEG files.

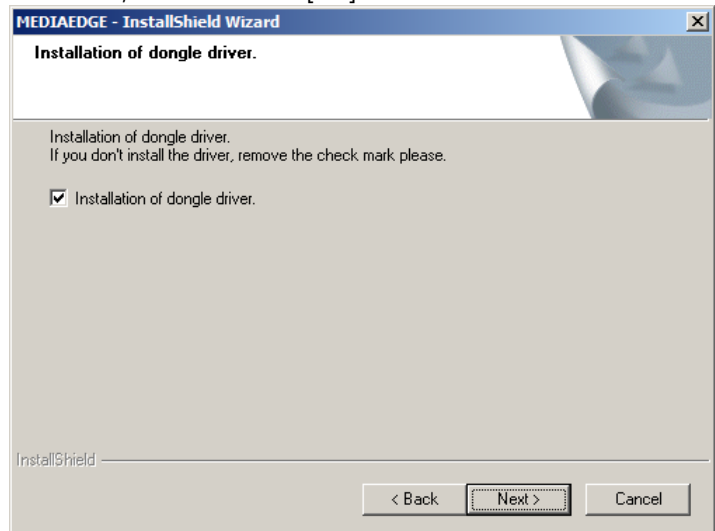


[10] Set the folder for installing the sample contents, and then click [Next].

The sample MPEG files will be copied to the folder that you specify here.

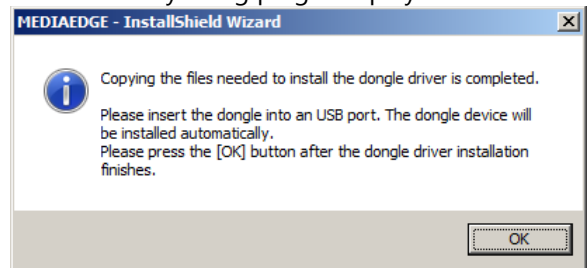


[11] Select the [Installation of dongle driver] check box, and then click [OK].



[12] When the dongle connection prompt message appears, connect the dongle to a USB port.

=> When the dongle is connected, the driver is installed automatically using plug and play.

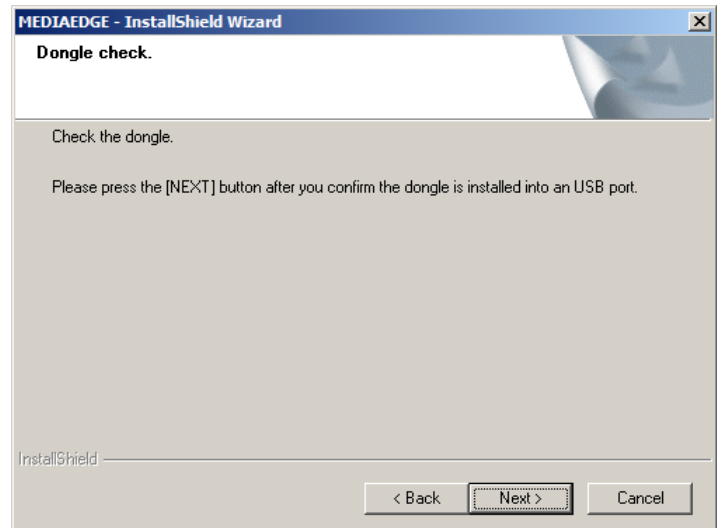


[13] After the dongle driver installation is complete, click [OK].

=> Continue with the following steps while the dongle is still connected

[14] Click [Next].

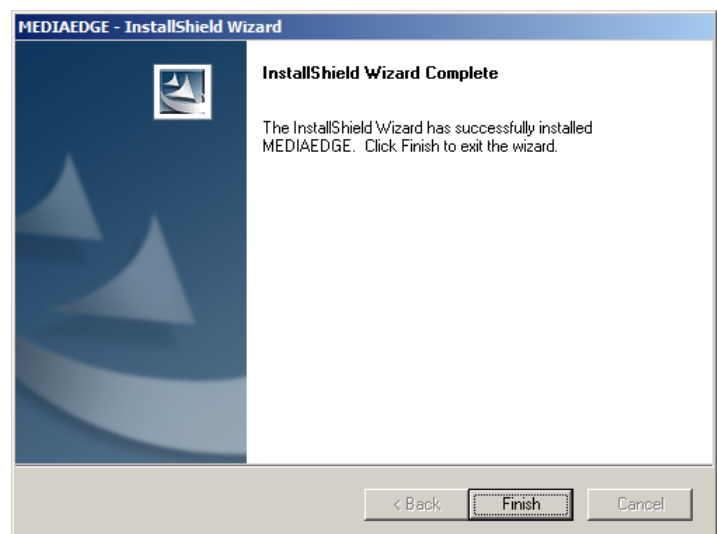
=> The installation starts.



[15] To view the release notes, click [Yes].

Be sure to read the release notes immediately after installation, because they contain information that is not in the manual.

[16] Click [Finish].



Checking operation after installing the MEDIAEDGE server

See [Chapter 2 3. Connecting to clients] in [MEDIAEDGE-SVS4 User's Guide], See [Chapter 2 3. Connecting to clients] in [MEDIAEDGE-SVS4 User's Guide], and check whether the sample video content can be played on the client devices, such as the STB4 or SWT4.

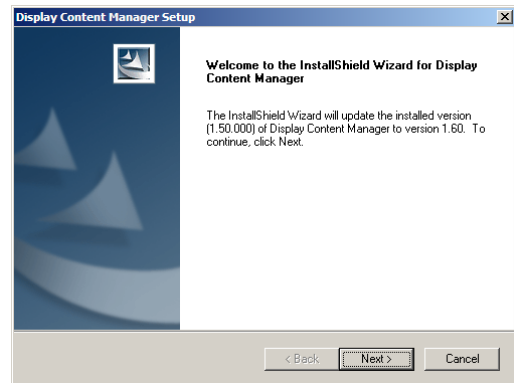
II-5. Display Content Manager Version Upgrade

This section describes the procedure for installing a new version of Display Content Manager to the computer in which an old version is installed.

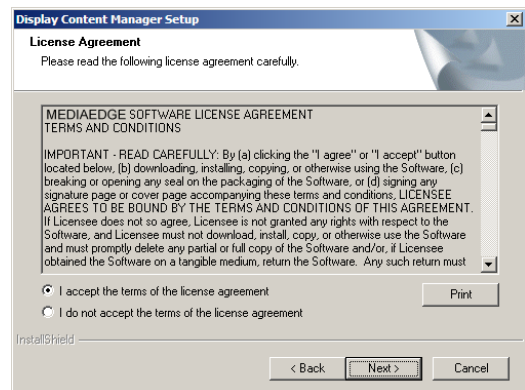
About the Display Content Manager version upgrade

The DCM must be upgraded on all computers on which the DCM system components are installed, such as the operation PC, DCM server and MEDIAEDGE server. (Upgrade process can be in any order.)

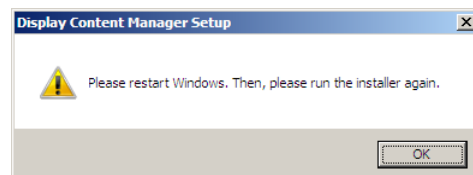
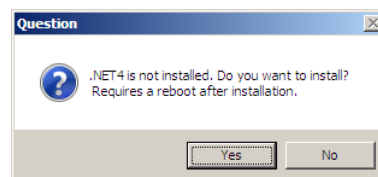
1. Insert the [Display Content Manager Installation Disc] into the DVD-ROM drive.
2. In the DVD-ROM drive, open the [DCM] folder and double-click [Setup.exe].
3. Click [Next].



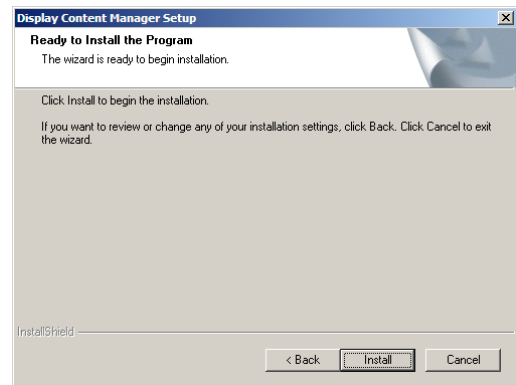
4. Select [I accept the terms of the license greement], and click [Next].



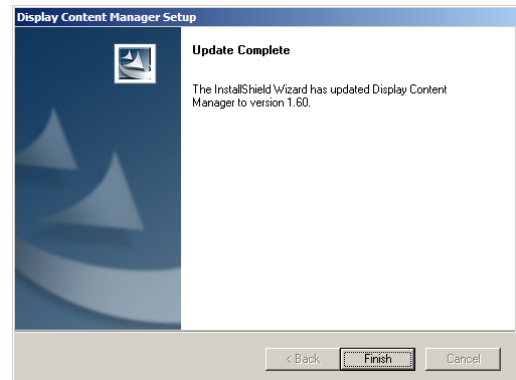
5. Click [Yes].
Install IIS, DotNet Framework 4.5 is started. It takes about 5 minutes.
6. Click [OK]. Then, please **restart** the OS.
After restarting, follow the procedure [1]-[4] again, and then go to the procedure



7. Click [Install].
=> The installation starts.
It takes about 10 minutes.



8. This completes the installation.
There are cases where the response of the system slows down immediately after installation. Please wait.



II-6. To secure the DCM system

Following user accounts will be created automatically along the DCM installation.

[1] MeDcmUser : The windows user account will be created to authenticate connections to the FTP server and Web server. This user account will be created when installing DCM server feature and FTP configuration at a time. (Default password 7ujM6yhN)

[2] MeOperator : The windows user account will be created to authenticate communications between DCM systems (except for database connection). This user account will be created when installing DCM server feature. (Default password !QAZxdr5)

[3] DcmOperator : The SQL Server user account will be created to authenticate connections to the database. This user account will be created when installing DCM server feature. (Default password 7ujM6yhN)

Immediately after installation, these user accounts have default password, on the other hand, the components of the DCM system use these default passwords to authenticate until the password is set. This is in order to save the trouble at operation checks, so you should change these passwords before official operation to secure the system. Especially, be sure to change the passwords if the DCM server will be located in the Internet

II-6-1. Change the MeDcmUser's password

[1] From the [Start] menu, open [Control Panel] and click [System and Security] and then click [Administrative Tools]. Next, double-click [Computer Management].

=> [Computer Management] opens.

* Please run in the DCM server.

* The above illustration is in the case of Windows Server 2008 R2. For the other OSes, please open the [Computer Management] in the same procedure.

[2] From the tree, display [Computer Management (Local)]->[System Tools]->[Local Users and Groups]->[Users].

[3] Right-click [MeDcmUser] and click [Set Password...].

[4] Click [Proceed].

[5] Enter [New password] and [Confirm password], then click [OK].

[6] From the [Start] menu, select [All Programs]->[MEDIAEDGE]->[DisplayContentManager], and click [DCMConsole], then select [Option] from the menu bar and click [FTP server...].

=> [FTP Server list] opens.

* Please run at an arbitrary operation PC with [DCM Application] has been installed.

* Please follow the procedure only once even if there is more than one operation PC.

[7] Select the FTP server which the password was changed, and click [Edit...].

[8] Enter [Password] and click [OK]

#Password : the password which was set at [5]

[9] Confirm that the message [FTP server connection succeeded] appears. then click [OK].

[10] Click [Close].

II-6-2. Change the MeOperator's password (DCM server)

[1] From the [Start] menu, open [Control Panel] and click [System and Security] and then click [Administrative Tools]. Next, double-click [Computer Management].

=> [Computer Management] opens.

* Please run in the DCM server.

* The above illustration is in the case of Windows Server 2008 R2. For the other OSes, please open the [Computer Management] in the same procedure.

[2] From the tree, display [Computer Management (Local)]->[System Tools]->[Local Users and Groups]->[Users].

[3] Right-click [MeOperator] and click [Set Password...].

[4] Click [Proceed].

[5] Enter [New password] and [Confirm password], then click [OK].

[6] From the [Start] menu, select [All Programs]->[MEDIAEDGE]->[DisplayContentManager], and click [DCM Configuration Tool], then move to [Server Connection]

* Please run at an arbitrary operation PC with [DCM Application] has been installed.

* Please follow the procedure only once even if there is more than one operation PC.

[7] Enter [Username] and [Password], then click [Connection Verification] and confirm that the message [Connection succeeded] appears.

#Server name : the host name of the DCM server

#IP Address : the IP address of the DCM server

#Username : MeOperator

#Password : the password of the above user

* When "IP Address" is omitted, "Server name" is used to connect to the DCM server.

* When "Username" and "Password" are blank, the default values are used.

[8] Click [OK] to close [DCM Configuration Tool].

[9] If you would like to deliver contents via the Internet, please configure the HDMA-4100 according to the following:

[IV-6-2. Set up ME-DEC, HDMA-4100 (if deliver contents via the Internet)]

II-6-3. Change the MeOperator's password (DCM add-on for SVS)

[1] From the [Start] menu, open [Control Panel] and click [System and Security] and then click [Administrative Tools]. Next, double-click [Computer Management].

=> [Computer Management] opens.

* Please run in the MEDIAEDGE server.

* If there is more than one MEDIAEDGE server, please perform the steps [1] to [8] for each MEDIAEDGE server.

* The above illustration is in the case of Windows Server 2008 R2. For the other OSes, please open the [Computer Management] in the same procedure.

[2] From the tree, display [Computer Management (Local)]->[System Tools]->[Local Users and Groups]->[Users].

[3] Right-click [MeOperator] and click [Set Password...].

[4] Click [Proceed].

[5] Enter [New password] and [Confirm password], then click [OK].

[6] From the [Start] menu, select [All Programs]->[MEDIAEDGE]->[DisplayContentManager], and click [DCMConsole], then click [Target] from the navigation bar.

=> [Target] screen of [DCM Console] opens.

* Please run at an arbitrary operation PC with [DCM Application] has been installed.

* Please follow the procedure only once even if there is more than one operation PC.

[7] From the subtree of [ME-SVS server], select the [MEDIAEDGE server] which the password was changed. Then, enter [Account] and [Password] at property window in right-pane.

Account : MeOperator

Password : the password which was set at [5].

[8] From the menu, select [View] and click [Refresh], then confirm that the MEDIAEDGE server's [Status] becomes [Online].

II-6-4. Change the DcmOperator's password

[1] From the [Start] menu, select [All Programs]->[MEDIAEDGE]->[DisplayContentManager], and click [Database Configuration Tool].

=> [Database Configuration Tool] opens.

* Please run in the DCM server.

[2] Enter [Computer name], [Instance name], [Port number], [Catalog name], [User name] and [Password], then click [Connection Verification].

Computer name : the computer name of the DCM server or IP address

Instance name : the instance name of the database(sets blank to specify default instance).

Catalog name : enter "CANOPUSDCM_DB"

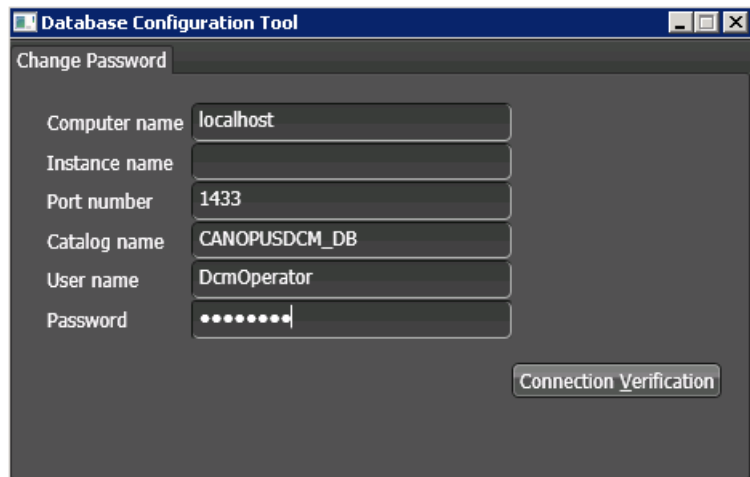
Port number : enter port number of the instance. (typically 1433 is used.)

User name : enter "DcmOperator"

Password : enter current password of SQL "DcmOperator" (*)

=> [Connection succeeded] message, [New Password] and [confirmation] input boxes, and [Change Password] button appear.

* Has been set to "7ujM6yhN" at installation as default.



Database Configuration Tool

Change Password

Computer name: localhost

Instance name:

Port number: 1433

Catalog name: CANOPUSDCM_DB

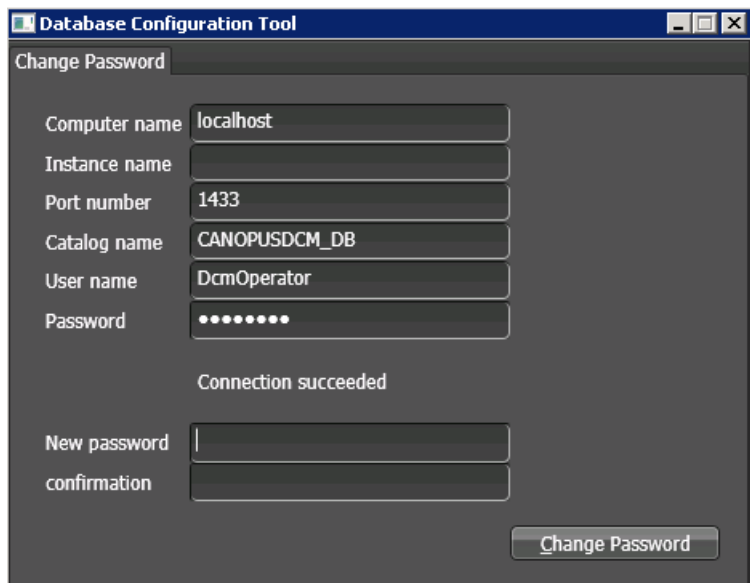
User name: DcmOperator

Password: ••••••••

Connection Verification

[3] Enter [New password], [confirmation], then click [Change password].

=> [Change password succeeded] appears.



Database Configuration Tool

Change Password

Computer name: localhost

Instance name:

Port number: 1433

Catalog name: CANOPUSDCM_DB

User name: DcmOperator

Password: ••••••••

Connection succeeded

New password:

confirmation:

Change Password

[4] Change the database connection according to following:

[IV-2-2. Settings for database connection]

III. Operation Checks

This chapter uses the samples that are stored on Display Content Manager to describe how to update the schedule for the playback clients.

III-1. Operation Checks

Select the products to be used.

If select the products to be used in the DCM configuration tool, DCM console provides easy operation. (Unwanted products will disappear.)

[1] From the [Start] menu, select [All Programs]->[MEDIAEDGE]->[Display Content Manager], and click [DCM Configuration Tool].

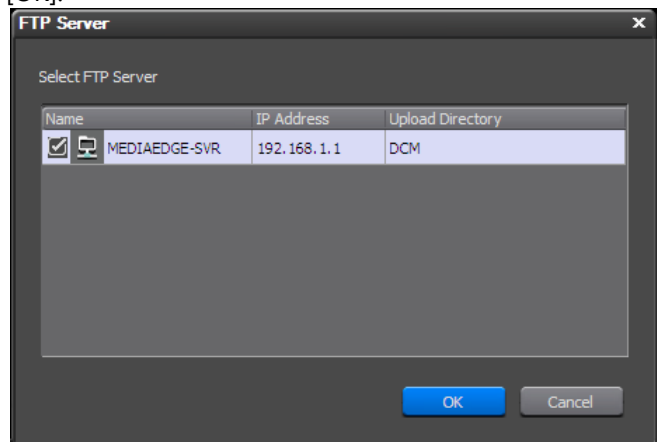
[2] Clear check box in the unused products, and then click [Apply].

III-1-1. Starting the DCM console

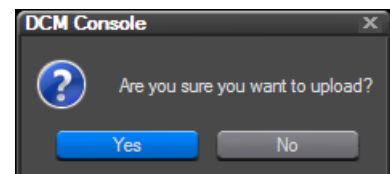
1. From the [Start] menu, select [All Programs]->[MEDIAEDGE]->[Display Content Manager], and click [DCM Console]. Alternatively, click the [DCM Console] shortcut on the desktop.
=> [DCM Console] opens.

III-1-2. Uploading content

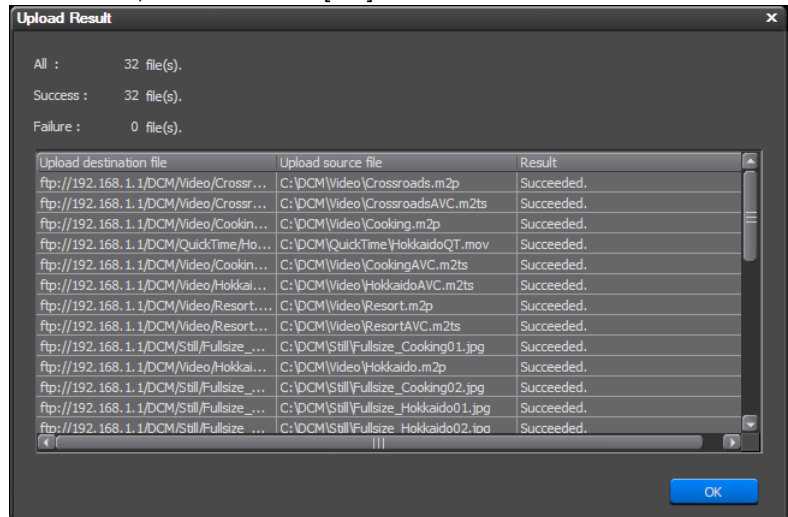
2. From the navigation bar, click [Material].
=> The [Content Window] is displayed.
3. From the menu bar, open [File]->[FTP] and click [Upload].
4. Select the FTP server check box, and then click [OK].



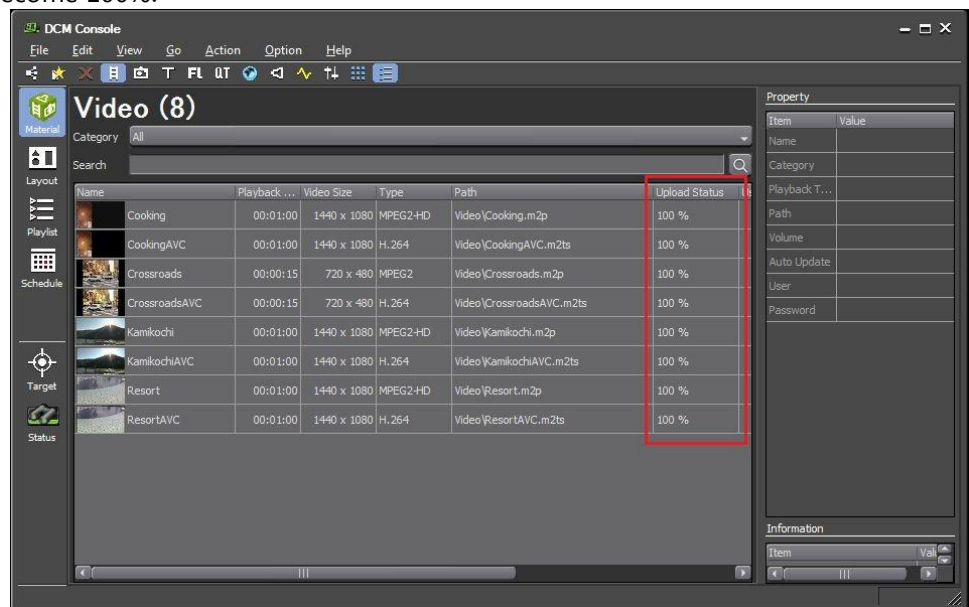
5. When the confirmation message appears, click [Yes].



- When uploading is complete, [Upload Result] opens. Check that the total number of uploads and the number of successful uploads are the same, and then click [OK].



- Upload status has become 100%.

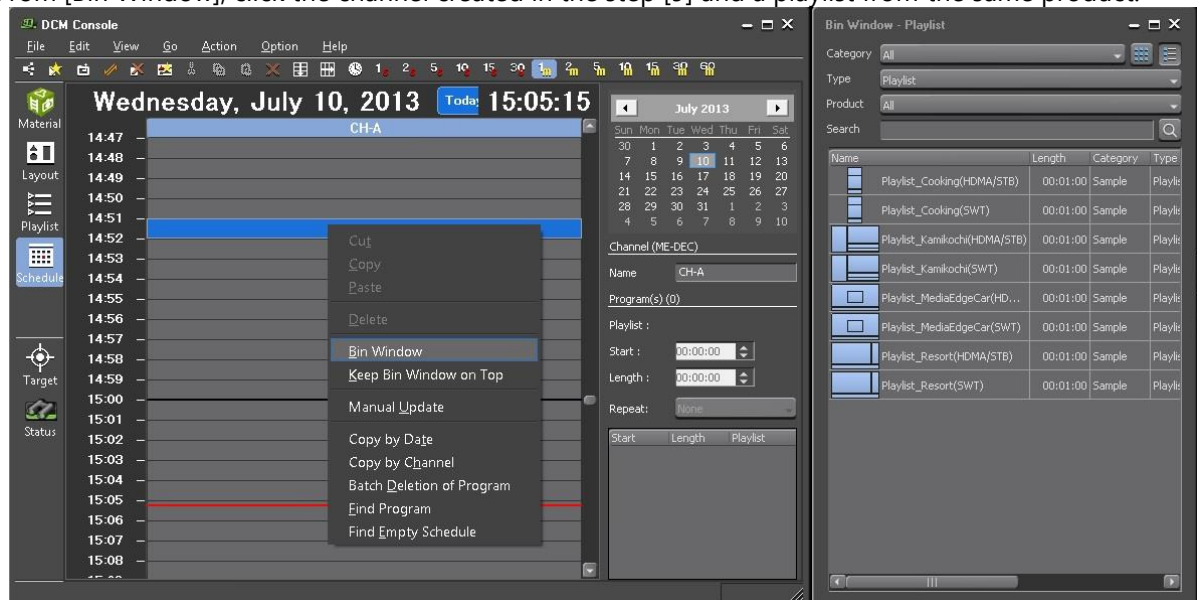


III-1-3. Schedule creation

8. From the navigation bar, click [Schedule].
=> The [Schedule Window] is displayed.
9. From the menu bar, open [File] and click [New].
=> [Create a new channel] opens
10. Enter a channel name, select the product, and then click [OK].
=> A channel is created.
11. From the menu bar, open [View] and click [Bin Window].
=> [Bin Window] opens



12. From [Bin Window], click the channel created in the step [9] and a playlist from the same product.



13. Click on the timeline of the channel.
=> The selected playlist is positioned on the timeline of the channel.

III-1-4. Target registration

1. From the navigation bar, click [Target].

Storage type (HDMA, ME-DEC)

2. Selects [Standalone Player] from the tree, then, [New] - [Group] to create a new group.

ME-SVS type

3. Selects [ME-SVS Server] from the tree, then [New] - [ME-SVS] to create a "ME-SVS"
4. Selects "ME-SVS" you created, and [New] - [Group] to create a new group

Name	Any name
Product	Group product type
ME-SVS Server	ME-SVS server created in step
Parent Group	None
Channel	Channel created
Command Channel	None

There are two ways to client registration

■ How to specify Cooperation with DCM (Automatic registration)

It uses the Client feature [Cooperation with DCM].

Specifies DCM server address to clients. Then the clients access the server and server side detects these. In this way, clients are available with DHCP.

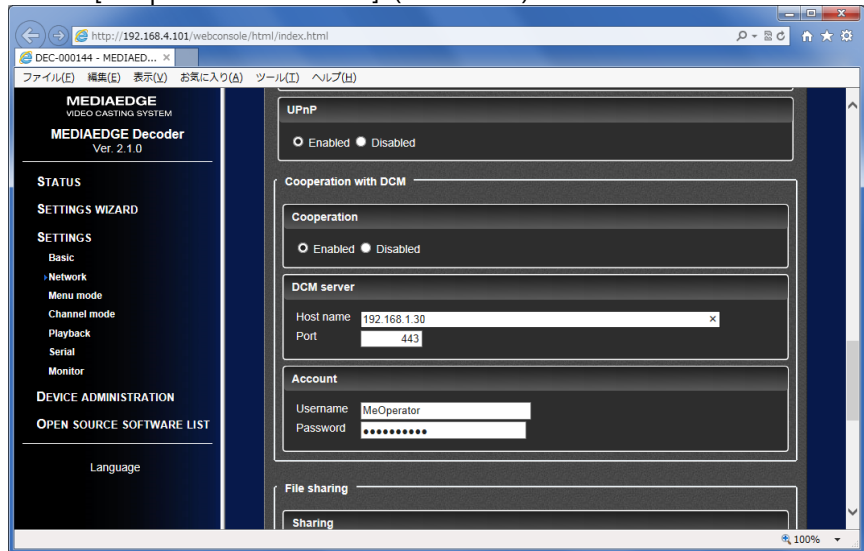
* ME-DEC, HDMA-4100 Ver2.0.0 or later is supported.

* SVS, STB, or SWT, is not available.

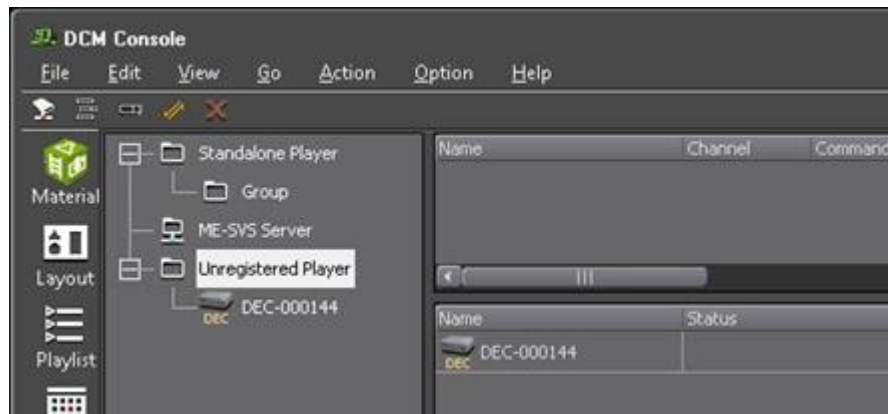
* DCM Console's [New] - [Client] is not used.

* You should use this way if you want to use DCM system via the Internet.

5. Set ME-DEC or HDMA-4100, feature [Cooperation with DCM]. (see IV-6-2)



6. Unregistered player will be displayed in the DCM console, and then drag & drop to the group you created

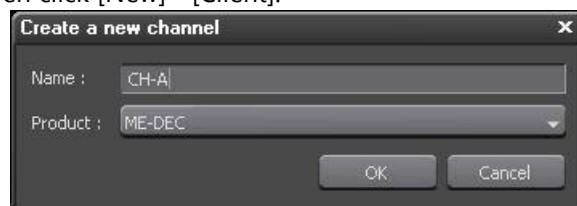


■ How to specify the IP address of the Client

In this way, do not use the [Cooperation with DCM].

7. Right-clicks the group you created from the tree, then click [New] - [Client].

Name	Any name
Group	Group registered
IP Address	IP address of client



Create a new channel

Name : CH-A

Product : ME-DEC

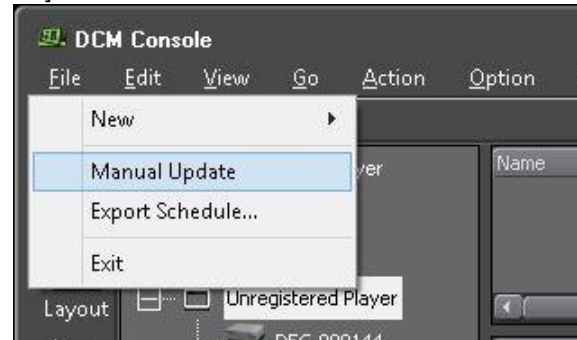
OK Cancel

III-1-5. Update operation

When it is updated

- * The DCM server makes schedule file and download.txt.
- * The DCM server sends download.txt to each client.
- * Each client downloads material files and the schedule file from FTP server (DCM).
- * Finally the schedule is downloaded, and playback is updated.

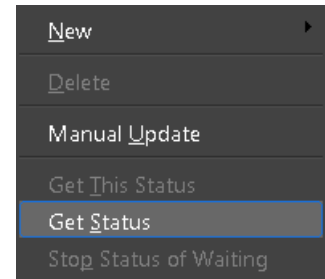
1. From the menu bar, open [File] and click [Manual Update].



2. Checks some groups which you want to update and click [OK].

III-1-6. Checking the update status

1. Please execute "Get Status" from right-click menu.



2. Please check the status.

Upper

Name	Group name
Channel	Channel assigned to a group (Required)
Command Channel	Command Channel assigned to a group
Days	Period of schedule to be updated (Max 365)
Programs	Number of programs contained in the schedule period.
File Size	Total size of files contained in the schedule period.
Last Update Start	Start date time of last update (manual and auto update)
Next Update Start	Start date time of next auto update * Update Start Time, Default 01:00 AM * If you do not use automatic updating, please input 9999 into [Update pattern].
Product	Group product type
Sub CH	Sub Channels *feature of ME-DEC or HDMA Ver2.1.2

Lower

Name	Client name
Status	Online : Communication has established Offline : Communication has not established (The device is not connected to the network, has no power, et al.) Shutdown : It is connected to the network, but has no power (Only ME-DEC)
IP address	IP address : IP address that has been set. Cooperation with DCM : IP address of the client. (Only display)
Capacity	Storage capacity.
Last Update Finish	Finished date time of last update.
Last Update Files	Number of files updated (successfully / Total)
Host name	Host name of the client. (Not be changed)
UID	Cooperation with DCM (Not be changed)
Description	Description of the client. (Not be changed)

Frequently problem

When HDMA, ME-DEC does not play even after the manual update, please check followings.

The DCM console [Options] - [FTP server], please set the IP address. When there is not DNS registration of the FTP server, ME-DEC or HDMA may need an IP address to access.

Please disable the firewall of DCM (FTP) server temporarily. Unintentionally, firewall rule might not work correctly.

Please set the date time of the ME-DEC or HDMA.

If the current time has not set correctly, the download process might not have completed in expected period. Also please take note of the time zone.

IV. Troubleshooting

This chapter describes the items that should be checked if the DCM system does not operate normally.

IV-1. Network Checks

The DCM system is comprised of the operation PC, FTP server, DCM server, MEDIAEDGE server, playback clients, and the network that connects all these devices.

IV-1-1. Communication within the DCM system

Within the DCM system, network communication must be possible.

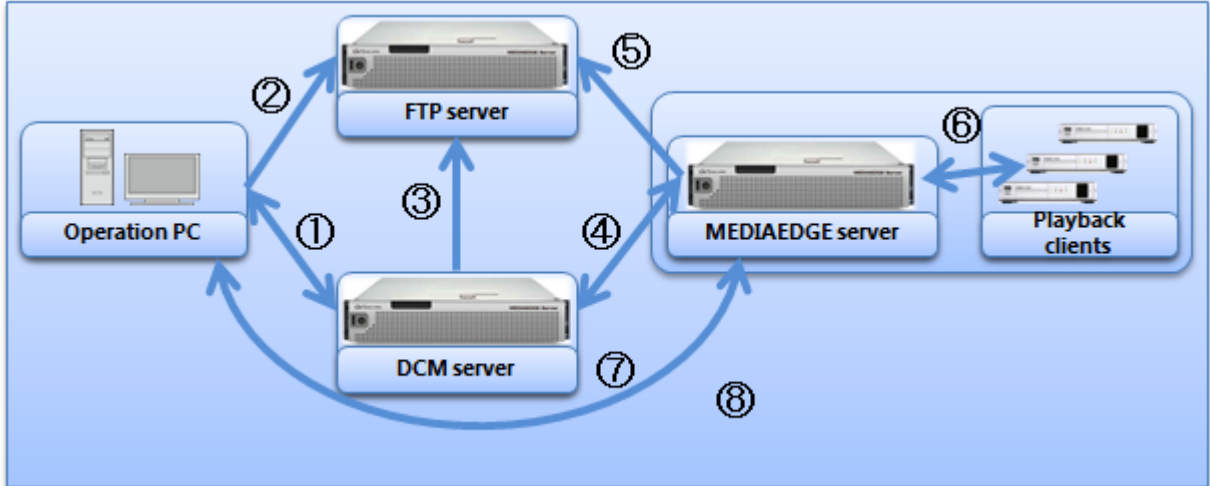


Fig. IV-1 Network connection in a DCM system that uses a MEDIAEDGE server

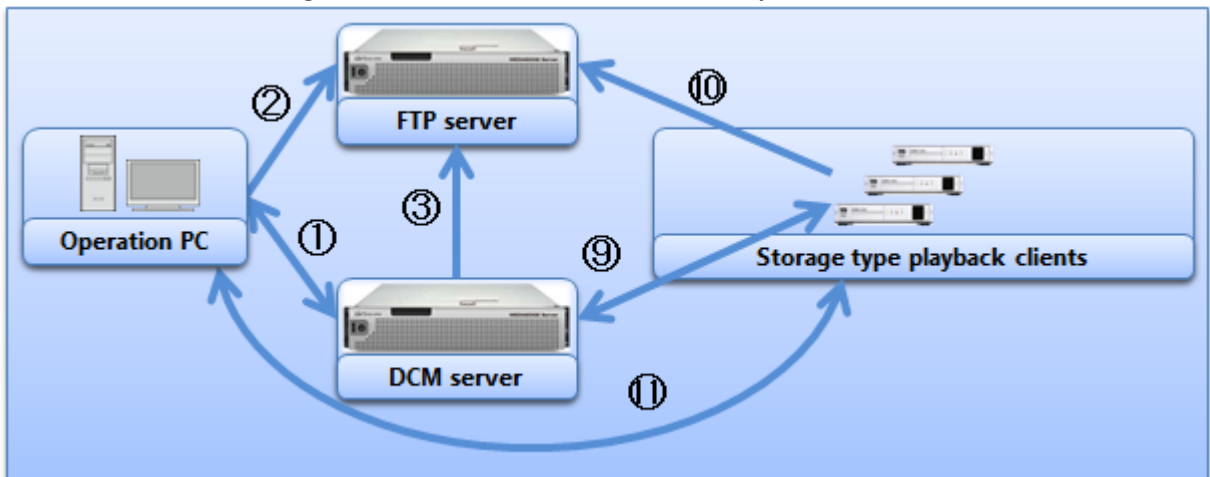


Fig. IV-2 Network connection in a DCM system that uses storage type playback clients

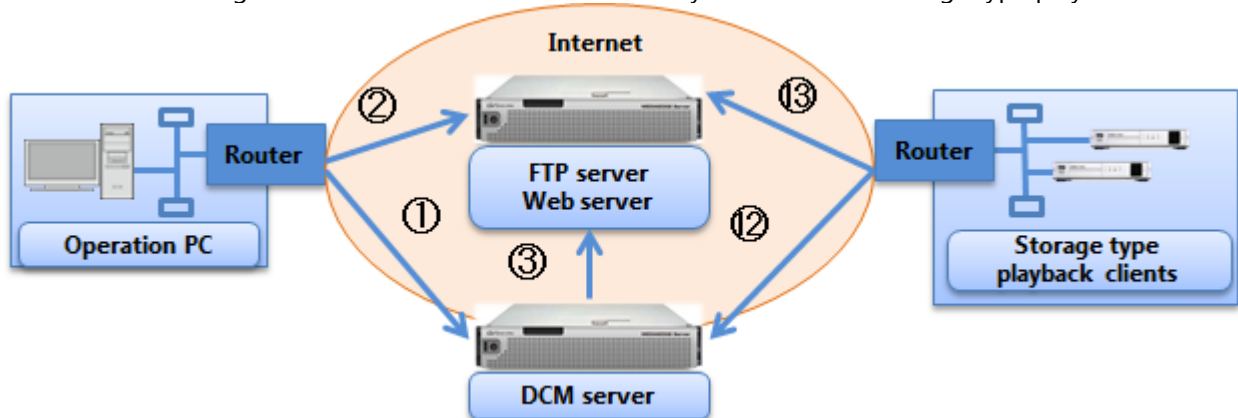


Fig. IV-3 Network connection in a DCM system via the Internet

(1) Operation PC -> DCM server

Service	Protocol	Receiving Port	Notes
HTTP	TCP	80	
SQL Server	TCP	1433, Unspecified	
	UDP	1434	
Samba	TCP	139,445	
	UDP	137,138	

(2) Operation PC -> FTP server

Service	Protocol	Receiving Port	Notes
FTP	TCP	21, Unspecified	

(3) DCM server -> FTP server

Service	Protocol	Receiving Port	Notes
FTP	TCP	21, Unspecified	

(4) DCM server -> MEDIAEDGE server

Service	Protocol	Receiving Port	Notes
HTTP	TCP	80	
Samba	TCP	139,445	
	UDP	137,138	

(5) MEDIAEDGE server -> FTP server

Service	Protocol	Receiving Port	Notes
FTP	TCP	21, Unspecified	

(6) MEDIAEDGE server -> Network type playback client

Service	Protocol	Receiving Port	Notes
DHCP	UDP	68	Only when used
DHCPv6	UDP	546	Only when used
HTTP	TCP	80	
RTP	UDP	STB = 1052,1054,1056,1058 SWT = Unspecified	
RTSP	TCP	554	
SNMP	UDP	161	Only when used
Serial Passthrough	TCP/UDP	Any port number	Only when used

MEDIAEDGE server <- Network type playback client

Service	Protocol	Receiving Port	Notes
DNS	TCP/UDP	53	Only when used
DHCP	UDP	67	Only when used
DHCPv6	UDP	547	Only when used
HTTP	TCP	80	
NTP	TCP/UDP	123	
RTSP	TCP	554	
SNMP	UDP	162	Only when used
Serial Passthrough	TCP/UDP	Any port number	Only when used

(7) Operation PC -> MEDIAEDGE server

Service	Protocol	Receiving Port	Notes
HTTP	TCP	80	
Samba	TCP	139,445	
	UDP	137,138	

(8) Operation PC -> Network type playback client

Service	Protocol	Receiving Port	Notes
HTTP	TCP	80	
SNMP	UDP	161	Only when used

(9) DCM server -> Storage type playback client

Service	Protocol	Receiving Port	Notes
DHCP	UDP	68	Only when used
DHCPv6	UDP	546	Only when used
HTTP	TCP	80	
Samba	TCP	139,445	
	UDP	137,138	

DCM server <- Storage type playback client

Service	Protocol	Receiving Port	Notes
DNS	TCP/UDP	53	Only when used
DHCP	UDP	67	Only when used
DHCPv6	UDP	547	Only when used
NTP	TCP/UDP	123	
SNMP	UDP	162	Only when used

(10) Storage type playback client -> FTP server

Service	Protocol	Receiving Port	Notes
FTP	TCP	21, Unspecified	

(11) Operation PC -> Storage type playback client

Service	Protocol	Receiving Port	Notes
HTTP	TCP	80	
SNMP	UDP	161	Only when used

(12) Storage type playback clients -> DCM server

Service	Protocol	Receiving Port	Notes
HTTPS	TCP	443	

(13) Storage type playback clients -> Web server

Service	Protocol	Receiving Port	Notes
HTTPS	TCP	443	

The simplest method for making all the connections from (1) to (11) is to configure all the devices in the same network segment.

For FTP communication [connections (2) (3) (5) (10)], because connection is obtained in passive mode, communication can be performed even if the FTP server is installed on an external network (such as the Internet).

If the DCM server is located in the Internet, the SQL Server communications [connections (1)] can be performed only if the port of SQL Server instance is fixed and set to enable the port. See followings section for more information.

=> [IV-2. Database Checks]

The HTTPS communication [connections (12) (13)] can be performed for ordinary network even if the server is located in the Internet.

For other communication [connections (4) (6) (7) (8) (9) (11)], a local network is required. Operation is not possible in networks called NAT and NAPT that convert the IP address and port number. For this reason, to configure a DCM system between points that are distant from each other, a local network must be constructed using technology such as VPN.

IV-1-2. Checking the network communication

Use the ping command to check the network reachability. From the computer's [Start] menu, select [All Programs]->[Accessories]->[Command Prompt] to check the network communication.

If the ping does not get through, check items such as the IP address that is assigned to each device, and the physical network cables. Also, check the following item.

[IV-13. Windows Firewall Settings]

After confirming there is a ping response and communication between the devices is enabled, see [III Operation Checks] and check whether the schedule update operation can be performed.

IV-2. Database Checks

If you cannot connect to the database, check the following items.

DCM server settings

[IV-2-1 TCP/IP settings for SQL Server]

[IV-13. Windows Firewall Settings]

DCM console settings

[IV-2-2 Settings for database connection]

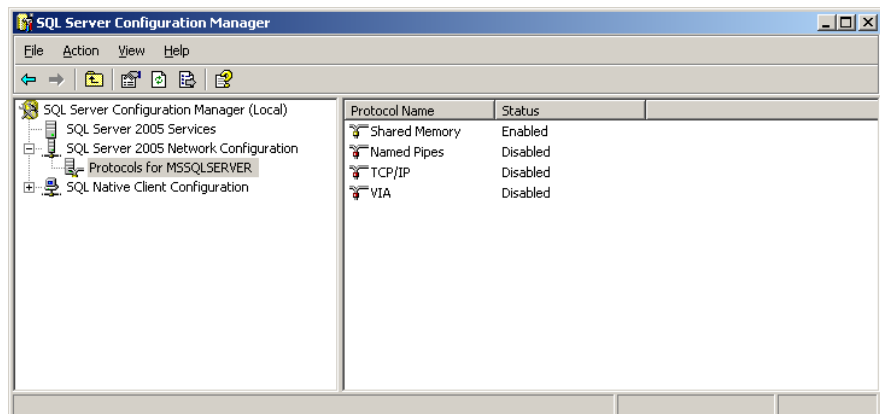
IV-2-1. TCP/IP settings for SQL Server

This section describes how to perform the settings for SQL Server that is installed on the DCM server.

[1] From the [Start] menu, select [All Programs]->[Microsoft SQL Server]->[Configuration Tools], and click [SQL Server Configuration Manager].

=> [SQL Server Configuration Manager] opens.

[2] From the tree, open [SQL Server Network Configuration] and click [Protocols for DB instance name](^{*1}).



^{*1}: DB instance name is the instance name of the database. If the instance name was set as blank during installation, MSSQLSERVER is displayed as the default instance name.

[3] Right-click [TCP/IP] and click [Enable].

[4] Right-click [TCP/IP] and click [Properties].

=> [TCP/IP Properties] opens.

[5] Click [IP Address] tab and check whether the value of [TCP Port] for [IP All] is set to 1433.

* If the Windows firewall is not disabled, add a rule to permit the TCP port number for the Windows firewall.

* If multiple instances exist, changing the TCP port number of a particular instance might affect other instances.

[6] Close [SQL Server Configuration Manager].

[7] From the [Start] menu, open [Control Panel]. Next, double-click [Administrative Tools], and then double-click [Services].

=> [Services] opens.

[8] Click [SQL Server (DB instance name)], and then click [Restart the service].

=> [SQL Server (DB instance name)] restarts and the setting changes are updated.

[9] Close [Services].

IV-2-2. Settings for database connection

Set the database connection information in the DCM configuration tool. The information set here is stored on the computer on which the configuration is performed. For this reason, the settings must be changed on all computers on which the DCM application is installed, such as the operation PC and DCM server.

[1] From the [Start] menu, select [All Programs]->[MEDIAEDGE]>[DisplayContentManager], and click [DCM Configuration Tool].

=> [DCM Configuration Tool] opens.

[2] Enter [Computer name], [Instance name], [Port] and [Authentication], and then click [Connection Verification].

=> Please verify that the "Connection succeeded." message is displayed.

Enter the computer name of the DCM server as the computer name. In a network environment that does not have a DNS server and cannot perform name resolution, enter the IP address of the DCM server.

Enter the name of the SQL Server instance as the instance name. Keep blank if the default instance (MSSQLSERVER) is being used.

Typically, enter 1433 for the port. If a value other than 1433 is set at [4-2-1. TCP/ IP settings for SQL Server], enter the value specified.

Choose either Windows authentication or SQL authentication. For authentication SQL, please enter your user name password.

IV-3. FTP Server Checks

If you cannot connect to the FTP server, check the following items.

FTP server settings

[IV-13. Windows Firewall Settings]

[IV-14. IIS Installation]

[IV-15. FTP Server Settings]

DCM console settings

[IV-3-1 Settings for FTP server connection]

IV-3-1. Settings for FTP server connection

Set the information for connecting to the FTP server in the DCM console. The information set here is stored in the database of the DCM server. For this reason, setting is only required for one computer, even if there are multiple computers on which the DCM application is installed. Be sure to reopen the DCM console on the computers on which the settings were not performed, in order to update them with the setting changes.

[1] Open the DCM console.

[2] From the menu bar, open [Option] and click [FTP Server].

=> [FTP Server list] opens.

[3] Select an FTP server and click [Edit].

=> [FTP Server Settings] opens.

[4] Enter access informations and click [Connection test]. After test has passed, click [OK].

* If you want to do [Connection test] only, click [Cancel] after confirmation.

Name	Computer name of the FTP server (DCM)
IP Address	IP address of the FTP server (DCM) If you omit [IP Address], which is accessed by using [Name]
Upload Directory	Directory name of the FTP server (folder name = DCM)
Account	An account on the FTP server (MeDcmUser)
Password	The password for the account (default button)

* IP Address is needed when DNS registration of the computer name is not carried out. ME-DEC, HDMA cannot access it even if Windows can access it. Please be careful.

IV-4. Web Server Checks

MIME settings of SMIL was set in MEDIAEDGE server where DCM add-on for SVS is installed. However, if the SMIL files on the MEDIAEDGE server cannot be browsed via HTTP(*2), the MIME settings of the Web server may have been erased. Check the settings as follows.

*2: They can be referred as URIs that the MEDIAEDGE server uses for redirecting playback clients. One example of them is

"http://MEDIAEDGE-SVR/DCM/smil/u.00000003_000000006.smil".

For details, see [IV-11-4 Messages related to the schedule].

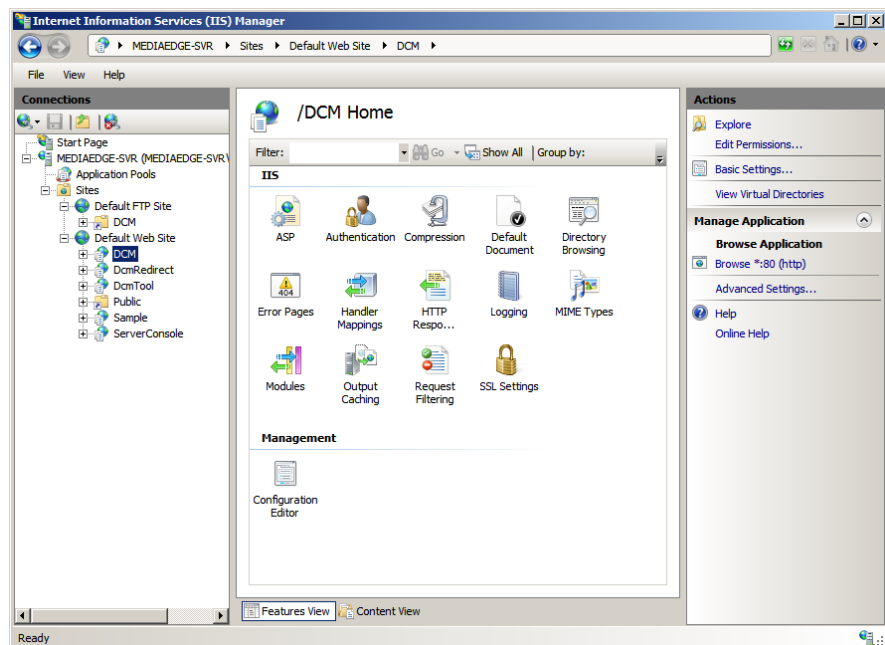
IV-4-1. MIME settings (Windows Server 2008 R2)

[1] From the [Start] menu, open [Control Panel] and click [System and Security] and then click [Administrative Tools]. Next, double-click [Internet Information Services (IIS) Manager].

=> [Internet Information Services (IIS) Manager] opens.

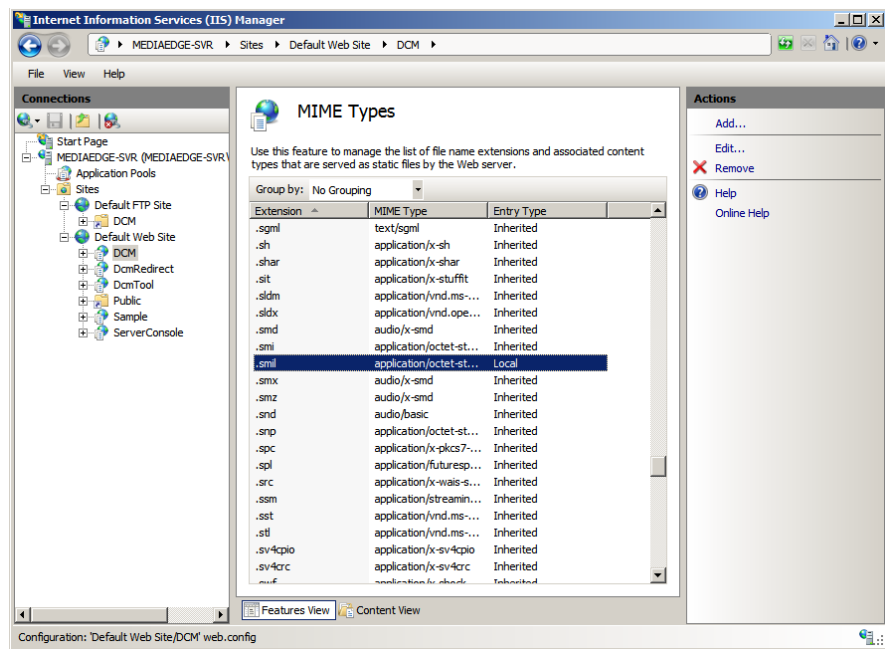
[2] From the tree, open [computer name(computer name\user name)]-> [Sites]-> [Default Web Site], and then click [DCM].

=> [/DCM Home] appears.



[3] Double-click [MIME Types].

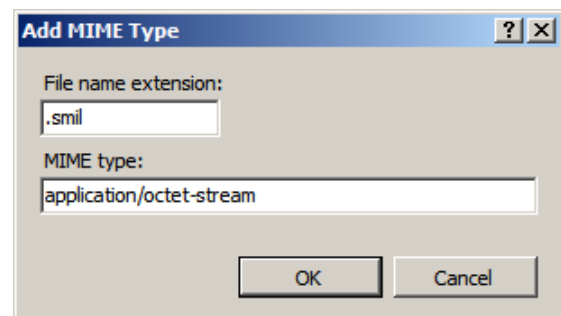
=> [MIME Types] appears.



[4] Check that [.smil] is registered in [Extension]. If [.smil] is not registered, click [Add]. Enter as follows.

File name extension : .smil

MIME type : application/octet-stream



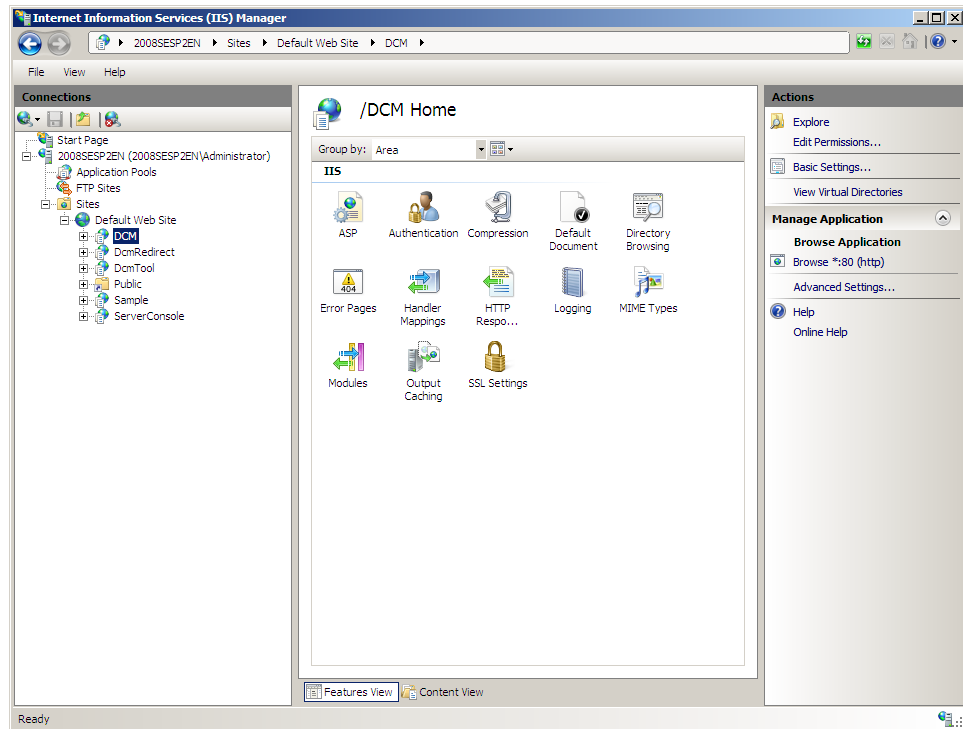
[5] Close [Internet Information Services (IIS) Manager].

IV-4-2. MIME settings (Windows Server 2008)

[1] From the [Start] menu, open [Control Panel] and click [Classic View]. Next, double-click [Administrative Tools], and then double-click [Internet Information Services (IIS) Manager].
=> [Internet Information Services (IIS) Manager] opens.

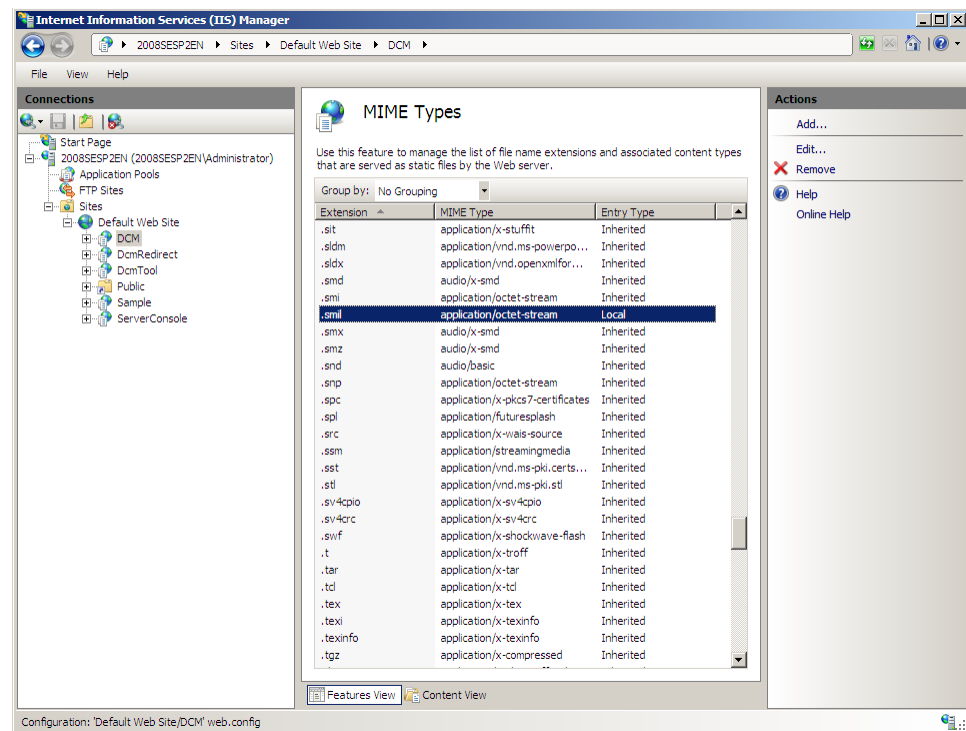
[2] From the tree, open [computer name(computer name\user name)]-> [Sites]-> [Default Web Site], and then click [DCM].

=> [/DCM Home] appears.



[3] Double-click [MIME Types].

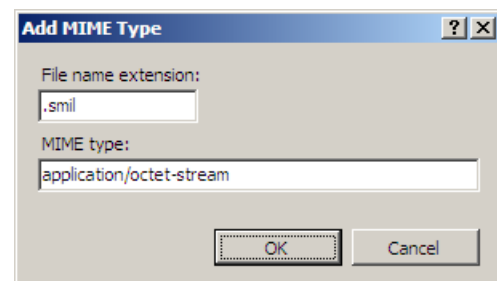
=> [MIME Types] appears.



[4] Check that [.smil] is registered in [Extension]. If [.smil] is not registered, click [Add]. Enter as follows.

File name extension .smil

MIME type application/octet-stream



[5] Close [Internet Information Services (IIS) Manager].

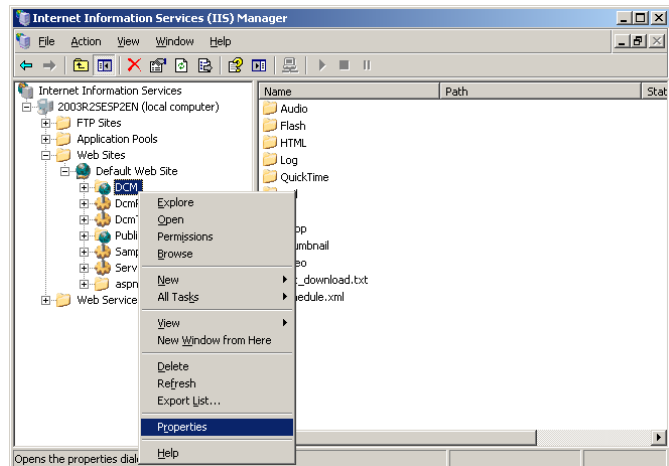
IV-5-3. MIME settings (Windows Server 2003 R2)

[1] From the [Start] menu, open [Control Panel]. Next, double-click [Administrative Tools], and then double-click [Internet Information Services (IIS) Manager].

=> [Internet Information Services (IIS) Manager] opens.

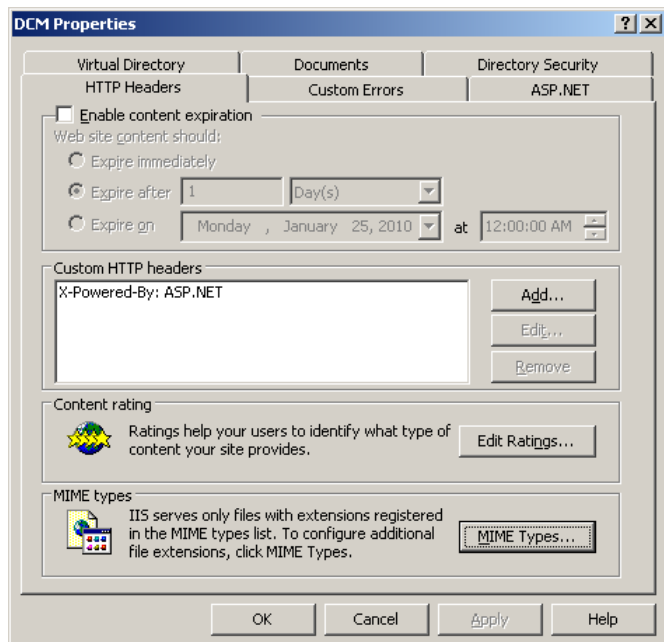
[2] From the tree, display [computer name (local computer)]->[Web Sites]->[Default Web Site]->[DCM]. Right-click [DCM] and click [Properties].

=> [DCM Properties] opens.

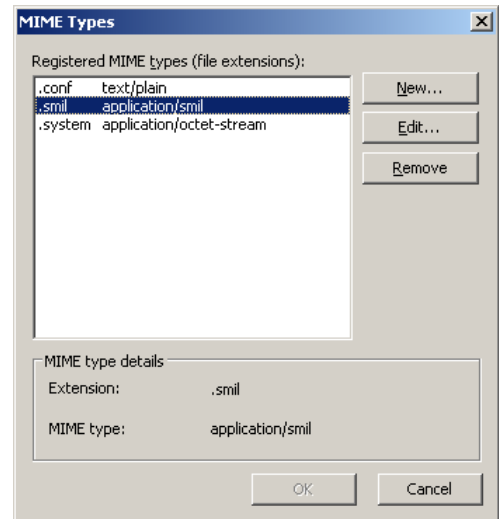


[3] Click [HTTP Headers], and then click [MIME Types].

=> [MIME Types] opens.



[4] Check that [.smil] is registered in [Extension].

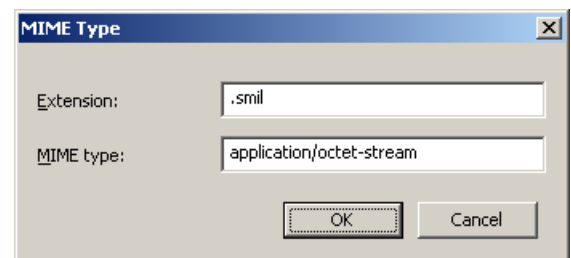


[5] If [.smil] is not registered, click [New].

Enter as follows.

File name extension .smil

MIME type application/octet-stream



[6] Close [Internet Information Services (IIS) Manager].

IV-5. NTP Server Settings

During the schedule update, the MEDIAEDGE server and storage type playback clients try to download the contents from the FTP server by an approximate update completion time that is specified in the download.txt file. The approximate update completion time is the time of the DCM server, but because the download itself is performed by the MEDIAEDGE server and the storage type playback clients, they must be set to the same time as the DCM server. They must also be set to the same time zone.

If you are not using an NTP server, adjust the time manually at regular intervals to prevent a large time divergence from occurring. To adjust the time automatically using the NTP server, check the following items.

IV-5-1. NTP server settings

This section describes how to set the NTP server. DCM ver.1.70 and later automatically configure the NTP server settings and the following steps are unnecessary.

[1] Change the following registry values.

(1) [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\w32time\Config]

"AnnounceFlags"=dword:00000005

(2) [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\w32time\TimeProviders\NtpServer]

"Enabled"=dword:00000001

[2] From the [Start] menu, open [Control Panel]. Next, double-click [Administrative Tools], and then double-click [Services].

=> [Services] opens.

[3] Restart the [Windows Time] service.

IV-5-2. NTP client settings

This section describes how to configure the NTP client of a computer where the MEDIAEDGE server or SWT is installed.

[1] Open [Date and Time] properties.

[2] Click [Internet Time], and then click [Change settings].

[3] Select the [Synchronize with an Internet time server] check box, and enter the name or IP address of the NTP server computer in [Server].

[4] Click [Update now], and after confirming that time synchronization can be performed, click [OK].

[5] Close [Date and Time] properties.

For details on how to configure the NTP client of hardware playback clients such as STB and HDMA, see the Web Console settings in the manual for each product.

IV-6. Playback Client Settings

IV-6-1. Samba shared settings for storage type playback clients

When using HDMA as a storage type playback client, the user name and password for accessing the Samba shared folder must be the same as the factory settings. If the user name and password have been changed, restore them to the factory settings. Also, Samba sharing must be set to [Use]. If the setting has been changed to [Do not use], set it to [Use].

** In case of ME-DEC, these Samba shared settings are unnecessary.*

The factory settings are as follows.

- ME-DEC
 - User name mediaedge
 - Password none
- HDMA-4100
 - User name mediaedge
 - Password hdp
- HDMA-4000
 - User name HDMA-4000
 - Password hdp

When using SWT as a storage type playback client, access the Samba shared folder that is created by the installer using the user and password that are created by the installer. Do not delete the following users or shared folders, or change the privileges.

The users and shared folders that are created on the computer on which SWT is installed are as follows.

- SWT4
 - User name ME-SWT-DS
 - Shared folder content
- SWT3 DS
 - User name ME-SWT-DS
 - Shared folder content

IV-6-2. Set up ME-DEC, HDMA-4100 (if deliver contents via the Internet)

If you would like to deliver contents via the Internet, samba shared settings of previous section are not necessary. Alternatively, set the followings settings to do cooperation with DCM:

- DCM server : Enabled
- Host name : Fully Qualified Domain Name of DCM server or IP address.
- Port number : 443
- User name : MeOperator
- Password : (*3)

**3: MeOperator's password which has been set at [II-8-2. Change the MeOperator's password (DCM server)]. Default password is !QAZxdr5.*

If using a proxy server is required for Internet connection, set the followings as well:

- Proxy server : host name or IP address of the proxy server
- Port (Proxy server) : port number of the proxy server for HTTPS connections

IV-7. Settings Required When Not Using a DNS Server

In a network environment that does not have a DNS server and cannot perform name resolution, directly enter the IP address for the following items.

- ◆ [III-1-4 Target registration]
- ◆ [III-2-4 Target registration]
- ◆ [IV-2-2 Settings for database connection]
- ◆ [IV-3-1 Settings for FTP server connection]
- ◆ [IV-5-2 NTP client settings]
- ◆ [IV-6-2. Set up ME-DEC, HDMA-4100 (if deliver contents via the Internet)]
- ◆ [IV-7-1 Settings for MEDIAEDGE server]

IV-7-1. Settings for MEDIAEDGE server

In the case of operations using MEDIAEDGE server, the playback clients must be able to connect to the MEDIAEDGE server. If the DNS server does not exist, do the following steps to change the MEDIAEDGE server settings;

[1] From the [Start] menu, select [All programs]->[MEDIAEDGE]-[DisplayContentManager], then click [DCM configuration tool].

=> [DCM configuration tool] opens.

[2] Move to [Others] screen.

[3] Double-click the MEDIAEDGE server to be set in [Each server settings], then enter the IP address of MEDIAEDGE server and click [Settings].

* If MEDIAEDGE server has multiple network interfaces, enter the IP address of an interface to which the playback clients are connected.

IV-8. Scheduled Serial Command Settings

If you want to use the scheduled serial command, you need to configure the devices in advance.

IV-8-1. MEDIAEDGE server and STB Settings

If your system consists of the STB and MEDIAEDGE server, configuration is required on both the MEDIAEDGE server and STB. (SWT playback client does not support the scheduled serial command.)

[1] STB settings

Set the serial mode from the Web Console in STB.

- Remote serial
"Connect to the following host" is selected, and enter the computer name or IP address of the MEDIAEDGE server associated with the STB.
- Host port number
60001 or any port number
- Listening port number
60001 or any port number
- Protocol
UDP or TCP
- Other settings
Set Baud rate, Data bits, Parity and Stop bits according to the controlled device.

Local settings

SYSTEM	NETWORK	SERIAL
MONITOR	VOD MODE	APPLY

Remote serial

- ☐ Disabled
- ☐ Connect to the streaming server
- ☒ Connect to the following host
- ☐ Work as a server

Host port number

Listening port number

Protocol ☐ TCP ☒ UDP

Baud rate

- ☐ 1200 ☐ 2400 ☐ 4800 ☒ 9600 ☐ 19200
- ☐ 38400 ☐ 57600 ☐ 115200

Data bits ☐ 7 ☒ 8

Parity ☒ None ☐ Odd ☐ Even

Stop bits ☒ 1 ☐ 2

Logging ☐ Enabled ☒ Disabled

[2] MEDIAEDGE server settings

By default MEDIAEDGE server uses the following protocol and ports. If you want to use non-default settings, after create the following registry, please restart the MeRd-Srv service.

32bit OS

[HKEY_LOCAL_MACHINE\SOFTWARE\Canopus\DisplayContentManager\Settings\MeRdSrv] "SerialProtocolType"="UDP" (or "TCP")

HostPort=60001 (or Any port number)

ClientPort=60001 (or Any port number)

64bit OS

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Canopus\DisplayContentManager\Settings\MeRdSrv]

"SerialProtocolType"="UDP" (or "TCP")

HostPort=60001 (or Any port number)

ClientPort=60001 (or Any port number)

IV-8-2. Storage type playback clients settings

Set the serial mode from the Web Console in ME-DEC or HDMA. (SWT playback client does not support the scheduled serial command.)

- Serial port function "Scheduled serial command" is selected
- Other settings Set Baud rate, Data bits, Parity, Stop bits and Flow control according to the controlled device.

The screenshot shows a web console titled "Local settings" with a dark blue header. Below the header is a table with four columns: SYSTEM, NETWORK, SCHEDULE, and SERIAL. The first row of the table contains the labels: PLAYBACK MODE, MONITOR, MENU MODE, and APPLY. Below the table, there are several configuration sections, each with a title and a list of radio button options:

- Serial port function**:
 - ☐ Disabled
 - ☐ Remote serial
 - ☐ Serial control
 - ☒ Scheduled serial command
 - ☐ Touch screen control
- Baud rate**:
 - ☐ 1200 ☐ 2400 ☐ 4800 ☒ 9600 ☐ 19200
 - ☐ 38400 ☐ 57600 ☐ 115200
- Data bits**:
 - ☐ 7 ☒ 8
- Parity**:
 - ☒ None ☐ Odd ☐ Even
- Stop bits**:
 - ☒ 1 ☐ 2
- Flow control**:
 - ☒ None ☐ Software (X-ON/X-OFF) ☐ Hardware (CTS/RTS)

IV-9. Ticker Content

IV-9-1. Encoding format for text files

In the settings after installation for this product (DCM Ver.1.10 or later), set the ticker content to output as a text file in [UTF-8 format with Byte Order Mark (BOM)]. Because some playback clients (HDMA-4000, HDMA-4000 Sync, STB3 DS) do not support text files in [UTF-8 format with BOM], their settings must be changed so that the text file is output as [ASCII format].

Setting method (*4)

To change the setting, create the registry as shown below for all the computers on which the DCM console is installed. Setting for outputting text files in [ASCII format]

**4 : When new ticker content is registered after setting the registry, a text file in the specified encoding format is created. Ticker content items that were registered before changing the settings can be updated to a text file in the specified encoding format by changing the string and uploading them to the FTP server.*

32bit OS

[HKEY_LOCAL_MACHINE\SOFTWARE\Canopus\DisplayContentManager\Settings\Material\Telop]
"CodePage"=dword:00000000

64bit OS

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Canopus\DisplayContentManager\Settings\Material\Telop]
"CodePage"=dword:00000000

To return the setting to outputting text files in [UTF-8 format with BOM], either set the registry as follows or delete. Setting for outputting text files in [UTF-8 format with BOM]

32bit OS

[HKEY_LOCAL_MACHINE\SOFTWARE\Canopus\DisplayContentManager\Settings\Material\Telop]
"CodePage"=dword:00000001

64bit OS

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Canopus\DisplayContentManager\Settings\Material\Telop]
"CodePage"=dword:00000001

- Playback clients that do not support text files in [UTF-8 format with BOM]
(Playback clients that can only display text files in [ASCII format])
 - HDMA-4000 Firmware Ver.3.1.3
 - HDMA-4000 Sync Firmware Ver.3.1.3
 - MEDIAEDGE-STB3 DS Firmware Ver.2.1.3
- Playback clients that can display text files in [UTF-8 format with BOM] and [ASCII format]
 - HDMA-4000 Firmware Ver.3.3.4 or later
 - HDMA-4000Sync Firmware Ver.3.3.4 or later
 - MEDIAEDGE-STB3 DS Firmware Ver.2.3.2 or later
 - HDMA-4100 Firmware Ver.1.4.9 or later
 - MEDIAEDGE-STB4 Firmware Ver.1.4.9 or later
 - MEDIAEDGE-STB4H Firmware Ver.1.4.9 or later
 - MEDIAEDGE-SWT3 DS Ver.1.00 (Release1) or later
 - MEDIAEDGE-SWT4 Ver.1.00 (Release1) or later

None of the playback clients support text files in [UTF-8 format without BOM].

IV-10. Log Files for MMSrv Service

Log files for the MMSrv service are output to the DCM server and MEDIAEDGE server.

IV-10-1. About log files for MMSrv service

Log files for the MMSrv service are output to the folder in accordance with the following output destination rule. If the MEDIAEDGE server is installed with [D:\DCM] specified as the work folder, it is output to the location of the output destination example.

- Output destination rule [(Work folder)\Log\(unique string that is created at installation)\MMSrv]
- Output destination example [D:\DCM\Log\FFFFFFFF-FFFF-FFFF-FFFFFFFFFFFFFFFF\MMSrv]

A log file is created each day in accordance with the following file name rule. A file created on December 8, 2009 would have the name shown in the file name example.

- File name rule [MMSrvyyyymmdd.log]
- File name example [MMSrv20091208.log]

The MMSrv service log is output in [ASCII format]. It can be opened with a text editor such as Notepad.

The log is comprised of 4 parts: date and time, priority, type and contents.

- Date and time
 - The date and time at which the log was recorded.
 - It is specified in YYYY-MM-DDThh:mm:ss.s TZD format (*5).
*5: Date and time format of W3C (<http://www.w3.org/TR/NOTE-datetime>)
- Priority
 - The log priority is expressed in 4 levels.
 - info Information
 - notice Notice
 - warning Warning
 - err Error
- Type
 - Logs are divided into the following types.
 - (None) Related to the operation of the MMSrv service
 - playlist Related to SMIL file creation
 - target Related to download.txt file creation
 - client Related to download operations
- Messages
 - Records log messages.

IV-10-2. Messages related to the operation of the MMSrv service

Log messages related to the operation of the MMSrv service is recorded with type = (None).

```
2009-12-08T14:11:01.769+09:00 info MMSrv was started
2009-12-08T14:11:50.927+09:00 info MMSrv was stopped
```

[MMSrv was started] is recorded when the service starts.

[MMSrv was stopped] is recorded when the service stops.

IV-10-3. Messages related to SMIL file creation

Log messages related to SMIL file creation is recorded with type = playlist by the MMSrv service that runs on the DCM server. Log messages after correct operations are as follows.

```
info playlist: transfer success [ftp://FTP-SVR/DCM/smil/0000000001.smil]
info playlist: transfer success [ftp://FTP-SVR/DCM/smil/0000000002.smil]
info playlist: transfer success [ftp://FTP-SVR/DCM/smil/0000000003.smil]
```

[transfer success] indicates that a playlist created with the DCM console has been uploaded to the FTP server as a SMIL file.

If there is no connection with the database of the DCM server, log messages are as follows.

```
err playlist: database query error
err playlist: database open error
```

[database query error] is recorded when there was a connection with the database, but the connection was broken. [database open error] is recorded when there was no connection with the database. Check the following item.

[IV-2 Database Checks]

If the SMIL file cannot be uploaded to the FTP server, log messages are as follows.

```
warning playlist: transfer failure [ftp://FTP-SVR/DCM/smil/0000000001.smil] (3304) [ftp://FTP-SVR/DCM/smil/0000000001.smil]
warning playlist: transfer failure [ftp://FTP-SVR/DCM/smil/0000000002.smil] (3304) [ftp://FTP-SVR/DCM/smil/0000000002.smil]
warning playlist: transfer failure [ftp://FTP-SVR/DCM/smil/0000000003.smil] (3304) [ftp://FTP-SVR/DCM/smil/0000000003.smil]
```

[transfer failure] records the file for which uploading failed. Use a browser such as Internet Explorer to check whether the file can be written to the directory (ftp://FTP-SVR/DCM/smil/, etc.) to which uploading was attempted.

Also, check the following item.

[IV-3 FTP Server Checks]

IV-10-4. Messages related to download.txt file creation

Log messages related to download.txt creation is recorded with type = target by the MMSrv service that runs on the DCM server.

If there is no connection with the database of the DCM server, log messages are as follows.

```
err target: database query error
err target: database open error
```

[database query error] is recorded when there was a connection with the database, but the connection was broken.

[database open error] is recorded when there was no connection with the database. Check the following item.

[IV-2 Database Checks]

Updating the schedule for MEDIAEDGE server

When the schedule is updated from the DCM server to the MEDIAEDGE server, log messages after correct operations are as follows.

```
info target: transfer success [ftp://FTP-SVR/DCM/schedule/00000003_00000005.xml]
info target: succeeded to put the download directive. [http://MEDIAEDGE-
SVR/mediaedge_api/version_1_0/control/contents_downloaded]
```

[1] First [transfer success]

=> Indicates that the schedule XML file (00000003_00000005.xml, etc.) was uploaded to the FTP server.

[2] Second [succeeded to put the download directive]

=> Indicates that the download.txt file was transferred via the MEDIAEDGE-API for the MEDIAEDGE server.

(Then, on the MEDIAEDGE server side, the required files start to be downloaded from the FTP server in accordance with download.txt file.)

Logs messages after the schedule XML file for the FTP server fails to upload are as follows.

```
warning target: transfer failure [ftp://FTP-SVR/DCM/schedule/00000003_00000005.xml] (3304) [ftp://FTP-
SVR/DCM/schedule/00000003_00000005.xml]
warning target: transfer failure [ftp://FTP-SVR/DCM/schedule/00000003_00000005.xml] (3304) [ftp://FTP-
SVR/DCM/schedule/00000003_00000005.xml]
warning target: transfer failure [ftp://FTP-SVR/DCM/schedule/00000003_00000005.xml] (3304) [ftp://FTP-
SVR/DCM/schedule/00000003_00000005.xml]
err target: cannot transfer Schedule.xml for MEDIAEDGE ( 5) [ MEDIAEDGE-SVR]
err target: cannot transfer download.txt for MEDIAEDGE [DCM]
```

[1] [transfer failure]

=> Records the schedule XML file for which uploading failed.

[2] [cannot transfer Schedule.xml for MEDIAEDGE]

=> Recorded when all upload operations fail after multiple retries.

[3] [cannot transfer download.txt for MEDIAEDGE]

=> Recorded when the download.txt file cannot be copied to the MEDIAEDGE server.

In this case, copying the download.txt file will result in an error regardless of whether or not the MEDIAEDGE server can be accessed. As such, first perform adjustments to enable uploading to the FTP server. Use a browser such as Internet Explorer to check whether the file can be written to the directory (ftp://FTP-SVR/DCM/schedule/, etc.) to which uploading was attempted. Also, check the following item.

[IV-3 FTP Server Checks]

When the download.txt file cannot be transferred to the MEDIAEDGE server even after the uploading the schedule XML file for the FTP server is successful, log messages are as follows.

Info target: transfer success [ftp://FTP-SVR/DCM/schedule/00000003_00000005.xml]

Warning target: failed to put the download directive. (500)[http://MEDIAEDGE-SVR/mediaedge_api/version_1_0/control/contents_downloaded]

Err target: cannot transfer download.txt for MEDIAEDGE [DCM]

[1] [transfer success] indicates that the schedule XML file was uploaded to the FTP server.

[2] [failed to put the download directive] indicates that the MEDIAEDGE-API on the MEDIAEDGE server cannot be accessed.

[3] [cannot transfer download.txt for MEDIAEDGE] is recorded when the download. txt file cannot be copied to the MEDIAEDGE server.

Check whether the MEDIAEDGE-API (http://MEDIAEDGE-SVR/mediaedge_api/version_1_0/, etc.) on the MEDIAEDGE server can be accessed.

Also, check the following item.

[III-1-4 Target registration]

Updating the schedule for storage type playback clients When the schedule is updated from the DCM server to storage type playback clients, log messages after correct operations are as follows.

```
info    target: transfer success [ftp://FTP-SVR/DCM/schedule/00000006_00000005.txt]
info    target: transfer success [¥¥192.168.1.101¥content¥download.txt]
info    target: transfer success [¥¥192.168.1.101¥content¥update.ctl]
```

[1] First [transfer success]

=> Indicates that the schedule TXT file (00000006_00000005.txt, etc.) was uploaded to the FTP server.

[2] Second [transfer success]

=> Indicates that the download.txt file was copied with Samba sharing for the storage type playback clients.

[3] Third [transfer success]

=> Indicates that the update.ctl file was copied with Samba sharing for the storage type playback clients. (Then, on the storage type playback client side, the required files start to download from the FTP server in accordance with download.txt file.)

Log messages after the schedule TXT file for the FTP server fails to upload are as follows.

```
Warning target: transfer failure [ftp://FTP-SVR/DCM/schedule/00000006_00000005.txt] (3304)
Warning target: transfer failure [ftp://FTP-SVR/DCM/schedule/00000006_00000005.txt] (3304)
Warning target: transfer failure [ftp://FTP-SVR/DCM/schedule/00000006_00000005.txt] (3304)
Err      target: cannot transfer Schedule.txt for HDMA group (5)
Err      target: cannot transfer download.txt for HDMA (5) [192.168.1.101]
```

[1] [transfer failure]

=> Records the schedule TXT file for which uploading failed.

[2] [cannot transfer Schedule.txt for HDMA group]

=> Recorded when all upload operations fail after multiple retries.

[3] [cannot transfer download.txt for HDMA]

=> Recorded when the download.txt file cannot be copied to the storage type playback clients.

In this case, copying the download.txt file will result in an error regardless of whether or not the shared folder of the storage type playback clients can be accessed. As such, first perform adjustments to enable uploading to the FTP server. Use a browser such as Internet Explorer to check whether the file can be written to the directory (ftp://FTP-SVR/DCM/schedule/, etc.) to which uploading was attempted.

Also, check the following item.

[IV-3 FTP Server Checks]

When the download.txt file cannot be copied to the storage type playback clients even after uploading the schedule TXT file for the FTP server is successful, log messages are as follows.
Note that a log related to the update.ctl file is not output.

```
Info      target: transfer success  [ftp://FTP-SVR/DCM/schedule/00000006_00000005.txt]
Warning   target: cannot open remote folder (35)  [¥¥192.168.1.101]
Err       target: cannot transfer download.txt for HDMA (5)  [192.168.1.101]
```

[1] [transfer success]

=> Indicates that the schedule TXT file was uploaded to the FTP server.

[2] [cannot open remote folder]

=> Indicates that the Samba shared folders on the storage type playback clients cannot be accessed.

[3] [cannot transfer download.txt for HDMA]

=> Recorded when the download.txt file cannot be copied to the storage type playback clients.

Check whether the Samba shared folder (\\192.168.1.101\content, etc.) on the storage type playback clients can be accessed.

Also, check the following items.

[III-2-4 Target registration]

[IV-6-1 Samba shared settings for storage type playback clients]

Updating the schedule for storage type playback clients (If deliver contents via the Internet)

When the schedule is updated from the DCM server to storage type playback clients, log messages after correct operations are as follows.

```
Info target: transfer success  [ftp://FTP-SVR/DCM/schedule/FTP-SVR/00000001_00000001.txt]
Info target: succeeded to put the download directive for the client (8)[HDMA- 050DE5]. [http://DCM-SVR/mediaedge_api/version_1_0/relay/control/ contents_download?target=00:21:11:05:0D:E5]
```

[1] [transfer success]

=> Indicates that the schedule TXT file was uploaded to the FTP server.

[2] succeeded to put the download directive for the client

=> Indicates that the download.txt file was transferred via HTTPS connection for the storage type playback clients.

Log messages after the schedule TXT file for the FTP server fails to upload are as follows.

```
Warning target: transfer failure  [ftp://FTP-SVR/DCM/schedule/FTP-SVR/00000001_00000001.txt] (3304)
[<ftp://FTP-SVR/DCM/schedule/FTP-SVR/00000001_00000001.txt>][Couldn't connect to server]0x7 [couldn't
connect to host]]
Warning target: transfer failure  [ftp://FTP-SVR/DCM/schedule/FTP-SVR/00000001_00000001.txt] (3304)
[<ftp://FTP-SVR/DCM/schedule/FTP-SVR/00000001_00000001.txt>][Couldn't connect to server]0x7 [couldn't
connect to host]]
Warning target: transfer failure  [ftp://FTP-SVR/DCM/schedule/FTP-SVR/00000001_00000001.txt] (3304)
[<ftp://FTP-SVR/DCM/schedule/FTP-SVR/00000001_00000001.txt>][Couldn't connect to server]0x7 [couldn't
connect to host]]
Err target: cannot transfer Schedule.txt for HDMA group (1)
Err target: cannot transfer download.txt for HDMA group (1) client (8)[HD MA-050DE5]]
```

[1] [transfer failure]

=> Records the schedule TXT file for which uploading failed.

[2] cannot transfer Schedule.txt for HDMA group

=> Recorded when all upload operations fail after multiple retries.

[3] cannot transfer download.txt for HDMA

=> Recorded when the download.txt file cannot be transferred to the storage type playback clients.

In this case, transferring the download.txt file will result in an error regardless of whether or not the storage type playback clients can be accessed. As such, first perform adjustments to enable uploading to the FTP server. Use a browser such as Internet Explorer to check whether the file can be written to the directory (ftp://FTP-SVR/DCM/schedule/. etc.) to which uploading was attempted. Also, check the following item.

[IV-3 FTP Server Checks]

When the download.txt file cannot be transferred to the storage type playback clients even after uploading the schedule TXT file to the FTP server is successful, log messages are as follows.

```
Info      target: transfer success[ftp://FTP-SVR/DCM/schedule/FTP-SVR/0000001_00000001.txt]
Warning   target: failed to put the download directive for the client(8) [HDMA-050DE5].(500) [ftp://DCM-
          SVR/mediaedge_api/version_1_0/relay/control/contents_downloaded?target=00:20:11:01:01:04]
err       target: cannot transfer download.txt for HDMA group (1) client (8) [HDMA-050DE5]
```

[1] [transfer success]

=> Indicates that the schedule TXT file was uploaded to the FTP server.

[2] [failed to put the download directive for the client]

=> Indicates that the connection for HTTPS was not established between the DCM server and the storage type playback clients.

[3] [cannot transfer download.txt for HDMA]

=> Recorded when the download.txt file cannot be transferred to the storage type playback clients.

Check the storage type playback clients settings:

[IV-6-2 Set up HDMA-4100 (if deliver contents via the Internet)]

IV-10-5. Messages related to download operations

Log messages related to download operations are recorded with type = client by the MMSrv service that runs on the MEDIAEDGE server. If Schedule.xml does not exist in the work folder "D:\DCM, etc.", a log message is as follows.

notice client: cannot set monitored client. missing [D:\DCM\Schedule.xml]

[cannot set monitored client] is recorded when Schedule.xml cannot be found. Recorded when there have not been any schedule updates for the MEDIAEDGE server from the DCM console, such as immediately after installing the DCM add-on for SVS onto the MEDIAEDGE server. This is not a malfunction.

When a download.txt file is created in the work folder of the MEDIAEDGE server, the updating (downloading from the FTP server) of the content files and schedule files is performed by the MMSrv service. Log messages are as follows.

* When delivering contents via the Internet, contents will be downloaded using HTTPS instead of FTP.

```

info    client:    download.txt is opened
info    client:    Download process start
info    client:    End time : 2009-12-08T17:13:56
info    client:    9 files in download.txt
info    client:    2 files already downloaded
info    client:    Download start : ftp://FTP-SVR/DCM/Video/HokkaidoAVC.m2ts
info    client:    Download success
info    client:    Download start : ftp://FTP-SVR/DCM/Video/HokkaidoAVC.m2ts.sha1
info    client:    Download success
info    client:    Download start : ftp://FTP-SVR/DCM/Still/Halfsize_Hokkaido.gif
info    client:    Download success
info    client:    Download start : ftp://FTP-SVR/DCM/Still/Halfsize_Hokkaido.gif.sha1
info    client:    Download success
info    client:    Download start : ftp://FTP-SVR/DCM/Telop/TickerHokkaido01.txt
info    client:    Download success
info    client:    Download start : ftp://FTP-SVR/DCM/Telop/TickerHokkaido01.txt.sha1
info    client:    Download success
info    client:    Download start : ftp://FTP-SVR/DCM/Telop/TickerHokkaido02.txt
info    client:    Download success
info    client:    Download start : ftp://FTP-SVR/DCM/Telop/TickerHokkaido02.txt.sha1
info    client:    Download success
info    client:    Download start : ftp://FTP-SVR/DCM/HTML/Hokkaido.html
info    client:    Download success
info    client:    Download start : ftp://FTP-SVR/DCM/HTML/Hokkaido.html.sha1
info    client:    Download success
info    client:    Download start : ftp://FTP-SVR/DCM/smil/0000000006.smil
info    client:    Download success
info    client:    Download start : ftp://FTP-SVR/DCM/smil/0000000006.smil.sha1
info    client:    Download success
info    client:    Content registered [c.00000007] [HokkaidoAVC]
info    client:    Channel registered [u.00000003.0] [STB4-Channel]
info    client:    Schedule registered [us.0000000e.00000022.0] []
info    client:    Schedule registered [us.0000000e.00000022.1] []
info    client:    Schedule registered [us.0000000e.00000022.2] []
info    client:    Download start : ftp://FTP-SVR/DCM/schedule/00000003_00000005.xml
info    client:    Download success
info    client:    7 files, 7 succeeded, 0 failed
info    client:    Download finished
info    client:    download.txt is deleted

```

The download operation is performed in the following sequence.

[1] [download.txt is opened]

=> The download.txt file is read.

[2] [Download process start]

=> The download process starts.

[3] End time : YYYY-MM-DDThh:mm:ss

=> Records the target time(*6) for the completion of downloading.

The update length is not a guaranteed value. If the transfer speed of the network line is not sufficient for the total transfer size, the target time may be exceeded.

Also, when a manual update is performed from the DCM console, because the current time is set as the target time, the computer tries to perform the download as quickly as possible.

*6 : Set based on the time of the DCM server. For this reason, if the time of the DCM server is further advanced than the time of the MEDIAEDGE server, updating may take some time. See [IV-6 NTP Server Settings] and set so that the time is adjusted automatically.

[4] [### files in download.txt]

=> Records the total number of files are written in the download.txt file.

It does not include the number of SHA1 files.

[5] [### files already downloaded]

=> If there are files already downloaded, records the number of those files.

=> If there are no files already downloaded, this log message is not recorded.

It does not include the number of SHA1 files.

[6] [Download start : ftp://FTP-SVR/DCM/dir/filename.ext][Download start : ftp://FTP-SVR/DCM/dir/filename.ext.sha1][Download success]

=> Indicates that the downloading of content files or SHA1 files has started.

=> Indicates that the downloading of the previous file was completed.

[7] [content registered]

[channel registered]

[schedule registered]

=> Indicates that content registration, channel registration and schedule registration onto the MEDIAEDGE server's database has been performed.

If no registrations have already been performed, this log message is not recorded.

[8] [Download start : ftp://FTP-SVR/DCM/schedule/NNNNNNNNN_NNNNNNNNN.xml][Download success]

=> Indicates that the downloading of the schedule XML file has started.

=> Also, indicates that the downloading was completed.

[9] [*N* files, *N* succeeded, *N* failed]

=> Records the number of files for which downloading was attempted, the number of successful downloads, and the number of failed downloads.

[10] [Download finished]

=> Indicates that the download operation was completed.

[11] [download.txt is deleted]

=> Indicates that the download.txt file has been deleted.

In fact, it is renamed to the file name: "last_download.txt".

If a file fails to download from the FTP server in download operation [6] or [8], log messages are as follows.

```
warning client: Download failure : ftp://FTP-SVR/DCM/Video/HokkaidoAVC.m2ts
warning client: Download failure : ftp://FTP-SVR/DCM/Still/Halfsize_Hokkaido.gif
warning client: Download failure : ftp://FTP-SVR/DCM/Telop/TickerHokkaido01.txt
warning client: Download failure : ftp://FTP-SVR/DCM/Telop/TickerHokkaido02.txt
warning client: Download failure : ftp://FTP-SVR/DCM/HTML/Hokkaido.html
warning client: Download failure : ftp://FTP-SVR/DCM/smil/0000000006.smil
warning client: cannot open SMIL document [D:¥DCM¥smil¥0000000006.smil]
warning client: cannot open SMIL document [D:¥DCM¥smil¥VOD_0000000006.smil]
warning client: Download failure : ftp://FTP-SVR/DCM/schedule/00000003_00000005.xml
info client: 7 files, 0 succeeded, 7 failed.
```

Use a browser such as Internet Explorer to check whether it is possible to download the files for which downloading failed. Also, check the following item.

[IV-3 FTP Server Checks]

If a connection cannot be made to the database of the MEDIAEDGE server in download operation [7], the log message is as follows.

```
Err client: database open error
```

IV-11. Log Files for MeRdSrv Service

Log files for the MeRdSrv service are output to the MEDIAEDGE server.

IV-11-1. About log files for MeRdSrv service

Log files for the MeRdSrv service are output to the folder in accordance with the following output destination rule. If the MEDIAEDGE server is installed with [D:\DCM] specified as the work folder, it is output to the location of the output destination example.

- Output destination rule [(Work folder)\Log\(unique string that is created at installation)\MeRdSrv]
- Output destination example [D:\DCM\Log\FFFFFFFF-FFFF-FFFF-FFFFFFFFFFFFFFFF\MeRdSrv]

A log file is created each day in accordance with the following file name rule. A file created on December 8, 2009 would have the name shown in the file name example.

- File name rule [MeRdSrvyyyymmdd.log]
- File name example [MeRdSrv20091208.log]

The MeRdSrv service log is output in [UTF-8 format with BOM]. It can be opened with a text editor such as Notepad.

The log is comprised of 3 parts: date and time, priority and message.

- Date and time
 - The date and time at which the log was recorded.
 - It is specified in YYYY-MM-DDThh:mm:ss.s TZD format(*7) .
 - *7: Date and time format of W3C (<http://www.w3.org/TR/NOTE-datetime>)
- Priority
 - The log priority is expressed in 4 levels.
 - ✧ info Information
 - ✧ notice Notice
 - ✧ warning Warning
 - ✧ err Error
- Message
 - Records log messages.

IV-11-2. Messages related to the operation of the MeRdSrv service

Log messages related to the operation of the MeRdSrv service is as follows.

```
2009-12-08T14:00:47.823+09:00 info Service Start Pending
2009-12-08T14:00:48.343+09:00 info Service Running
2009-12-08T14:43:46.442+09:00 info Service Stop Pending
2009-12-08T14:43:46.457+09:00 info Service Stopped
```

[Service Start Pending] is recorded when the service is starting.

[Service Running] is recorded after the service starts.

[Service Stop Pending] is recorded when the service is stopping.

[Service Stopped] is recorded after the service stops.

IV-11-3. Messages related to the client

Log messages related to the client is recorded when the MeRdSrv service starts or when the schedule is updated, and after Schedule.xml is read.

```
info    Schedule file is read. ScheduleFilePath="D:\DCM\Schedule.xml"
info    Clients Count=1 : Group= (3) STB4-Group
info    Client= (3) STB4-TestClient IPAddr=192.168.1.101 : Group= (3) STB4-Group
```

[1] [Schedule file is read.]

=> Records the path of the read Schedule.xml.

[2] [Clients Count]

=> Records how many playback clients belong to the client group. When there are multiple client groups, records on multiple lines.

[3] [Client]

=> Records the names of the playback clients, the IP addresses and the client groups to which they belong. If there are multiple playback clients, records on multiple lines.

IV-11-4. Messages related to the schedule

The MeRdSrv service instructs the playback clients of which playlist they should play by performing an operation called "redirecting" for the playback clients in accordance with the schedule. (The MEDIAEDGE server redirects the playback clients to the SMIL files.) Log messages related to the schedule records the redirect operations that are performed in client group units.

```

info    Set next schedule: Schedule= (5) 2009-12-08T15:00:00 Path= (8) http://MEDIAEDGE-
SVR/DCM/smil/u.000000003_0000000006.smil Group= (3) STB4-Group
info    Begin schedule redirect: Group= (3) STB4-Group info Set next schedule: Schedule= (5) 2009-12-
08T15:01:00 Path= (8) http://MEDIAEDGE-SVR/DCM/smil/u.000000003_0000000006.smil Group= (3)
STB4-Group
info    Begin schedule redirect: Group= (3) STB4-Group info Set next schedule: Schedule= (5) 2009-12-
08T15:02:00 Path= (8) http://MEDIAEDGE-SVR/DCM/smil/u.000000003_0000000006.smil Group= (3)
STB4-Group
info    Begin schedule redirect: Group= (3) STB4-Group
info    Set next schedule: Schedule=None Group= (3) STB4-Group

```

[1] [Set next schedule]

=> If there is a schedule later than the current time, records the schedule start time, the file path for the redirect destination and the target client group. If there is no schedule later than the current time, "None" is recorded.

[2] [Begin schedule redirect]

=> Indicates that the redirect operation started for the playback clients that belong to the client group.

(On the playback client side, playback starts after referring to the file path that is specified at the redirect destination. Check log messages

IV-11-5. Messages related to the command schedule

The MeRdSrv service sends commands for the playback clients in accordance with the command schedule. Log messages related to the command schedule records the command sending operations that are performed in client group units.

```

info  Set next command: CommandSchedule= (3) 2009-12-08T15:00:00 Command="%02PON%03" Group= (3)
      STB4-Group
info  Begin command execute: Group= (3) STB4-Group info Set next command: CommandSchedule= (4)
      2009-12-08T15:01:00 Command="%02PON%03" Group= (3) STB4-Group
info  Begin command execute: Group= (3) STB4-Group info Set next command: CommandSchedule= (5)
      2009-12-08T15:02:00 Command="%02PON%03" Group= (3) STB4-Group
info  Begin command execute: Group= (3) STB4-Group
info  Set next command: CommandSchedule=None Group= (3) STB4-Group

```

[1] [Set next command]

=> If there is a command schedule later than the current time, records the command schedule execution time, the command string and the target client group. If there is no command schedule later than the current time, "None" is recorded.

[2] [Begin command execute]

=> Indicates that the command sending started for the playback clients that belong to the client group.

(On the playback client side, commands are sent to the external device using serial passthrough. Check log messages on the playback client side. Note that the return value cannot be checked on the server.)

IV-12. download.txt Files

During an update operation, the download.txt file is distributed from the DCM server to the MEDIAEDGE server and storage type playback clients. The MEDIAEDGE server and storage type playback clients download the required number of files from the FTP server in accordance with the contents of the download.txt file.

IV-12-1. About download.txt files

The download.txt files are transferred in accordance with the following rule. After the download operation is completed, the file is renamed to last_download.txt.

- MEDIAEDGE server
 - Transferred by MEDIAEDGE-API (http://MEDIAEDGE-SVR/mediaedge_api/version_1_1/control/contents_download)
- HDMA
 - Copied to content folder by HDMA's file sharing feature.*8)

*8 : download.txt files that are output to the HDMA content folder are immediately moved to the playlist folder.
- HDMA (if deliver contents via the Internet)
 - Transferred by MEDIAEDGE-API (http://MEDIAEDGE-SVR/mediaedge_api/version_1_1/relay/control/contents_download)
- SWT
 - Copied to content folder by Windows's file sharing feature.

The download.txt file is output in [UTF-8 format without BOM]. It can be opened with a text editor such as Notepad.

```
version: 1.0
create: 2009-12-16T18:28:27.000+09:00
end: 2009-12-16T18:28:27.000+09:00
expire: 2009-12-25T00:00:00.000+09:00

download id=7 type=movie src="ftp://192.168.10.4/DCM/Video/HokkaidoAVC.m2ts"
dst="Video¥HokkaidoAVC.m2ts" user=Administrator password=admin size=76044288
hash=dummy_20090518T064902000000000000076044288
download id=19 type=still src="ftp://192.168.10.4/DCM/Still/Halfsize_Hokkaido01.jpg"
dst="Still¥Halfsize_Hokkaido01.jpg" user=Administrator password=admin size=164966
hash=dummy_20080714T10113000000000000000164966
download id=20 type=still src="ftp://192.168.10.4/DCM/Still/Halfsize_Hokkaido02.jpg"
dst="Still¥Halfsize_Hokkaido02.jpg" user=Administrator password=admin size=140085
hash=dummy_20080714T10114700000000000000140085
download id=21 type=still src="ftp://192.168.10.4/DCM/Still/Halfsize_Hokkaido.gif "
dst="Still¥Halfsize_Hokkaido.gif " user=Administrator password=admin size=43330
hash=dummy_20080422T02531200000000000000043330
download id=28 type=ticker src="ftp://192.168.10.4/DCM/Telop/TickerHokkaido01.txt"
dst="Telop¥TickerHokkaido01.txt" user=Administrator password=admin size=378
hash=dummy_20090521T0445350000000000000000378
download id=29 type=ticker src="ftp://192.168.10.4/DCM/Telop/TickerHokkaido02.txt"
dst="Telop¥TickerHokkaido02.txt" user=Administrator password=admin size=374
hash=dummy_20090521T0445190000000000000000374
download id=31 type=html src="ftp://192.168.10.4/DCM/HTML/Hokkaido.html" dst="HTML¥Hokkaido.html"
user=Administrator password=admin size=720 hash=dummy_20091013T063450000000000000000720
download id=37 type=smil src="ftp://192.168.10.4/DCM/smil/0000000006.smil" dst="smil¥0000000006.smil"
user=Administrator password=admin size=1817 hash=322136441ca7cd6db881ac11225342ac59c53051
download id=48 type=schedule src="ftp://192.168.10.4/DCM/schedule/00000003_00000005.xml" dst="Schedule.xml"
user=Administrator password=admin size=1109
```

```
content name="c.00000007" title="HokkaidoAVC" src="Video¥HokkaidoAVC.m2ts" length=60000
channel name="u.00000003" title="STB4-Channel" destination="0.0.0.0" count=1
schedule name="us.0000001a.0000001a" channel="u.00000003.0" content="c.00000007" base="2009-12-
16T19:15:00.000+09:00" last="2009-12-16T19:16:00.000+09:00" offset="0" duration="60" period="60"
```

[1] [version]

=> Specifies the version of download.txt.

[2] [create]

=> Specifies the date and time of download.txt creation.

[3] [end]

=> Specifies the target completion time for the schedule update (file download).

The update completion time is not a guaranteed value.

In a download.txt file that is created for an automatic update, a time is specified where the approximate update length is added to the update start time, and the download speed is adjusted accordingly.

In a download.txt file that is created from a manual update, the same time as the creation date and time is specified, and the download is performed at the highest speed.

[4] [expire]

=> Specifies the expiry date of download.txt. The download operation cannot be performed after this date and time has elapsed.

[5] [download]

=> Specifies the information about the file to be downloaded.

[6] [content]

=> Specifies the information for registering content on the MEDIAEDGE server.

[7] [channel]

=> Specifies the information for registering channels on the MEDIAEDGE server.

[8] [schedule]

=> Specifies the information for registering schedules on the MEDIAEDGE server.

IV-13. Windows Firewall Settings

IV-13-1. Firewall the installer set

The installer of DCM1.80 registers a firewall into a DCM server.

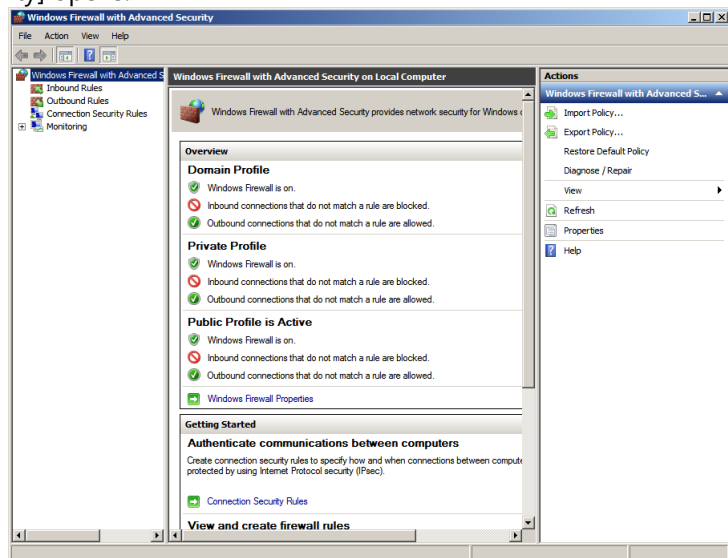
Name	Port
MEDIAEDGE (NTP)	UDP 123
MEDIAEDGE (SQL)	TCP 1443
MEDIAEDGE (HTTP)	TCP 80
MEDIAEDGE (HTTPS)	TCP 443
MEDIAEDGE (FTP)	Ftpsvc

The above firewall rules has been created during installation of DCM, though, unintentionally these rules might not work correctly. When such a case, please disable a firewall temporarily to check the operation. In this section, explains how to disable the firewall.

IV-13-2. Windows Server 2008 R2

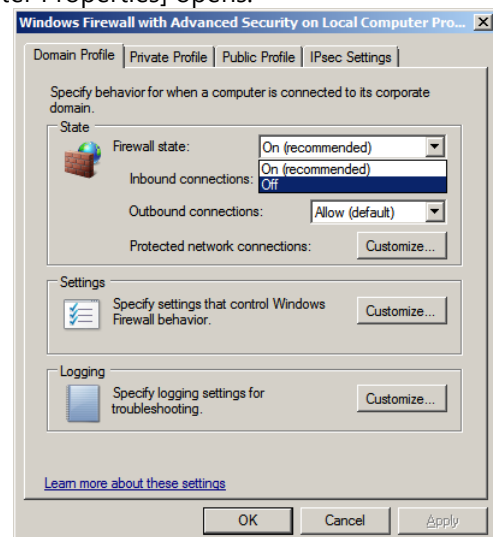
[1] From the [Start] menu, open [Control Panel] and click [System and Security] and then click [Administrative Tool]. Next, double-click [Windows Firewall with Advanced Security].

=> [Windows Firewall with Advanced Security] opens.



[2] Click [Windows Firewall Properties].

=> [Windows Firewall with Advanced Security on Local Computer Properties] opens.



[3] Click [Domain Profile] and set [Firewall state] to Off.

[4] Click [Private Profile] and set [Firewall state] to Off.

[5] Click [Public Profile] and set [Firewall state] to Off.

[6] Click [OK].

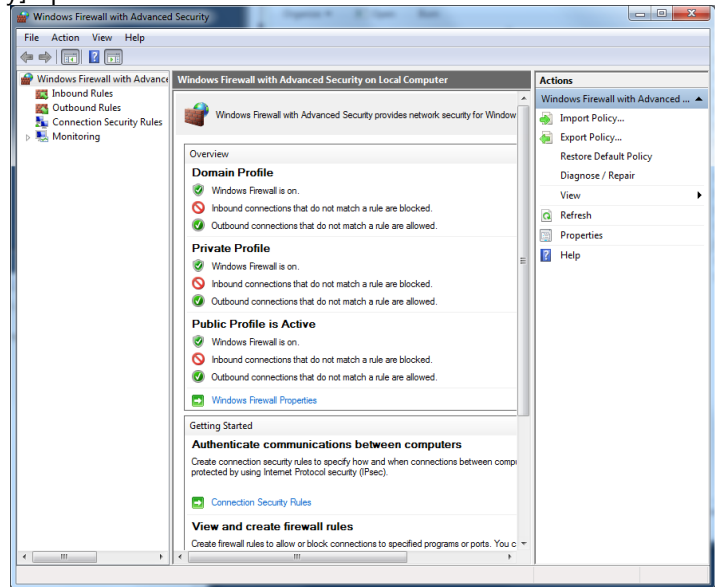
=> [Windows Firewall with Advanced Security on Local Computer Properties] closes.

[7] Close [Windows Firewall with Advanced Security].

IV-13-3. Windows 7

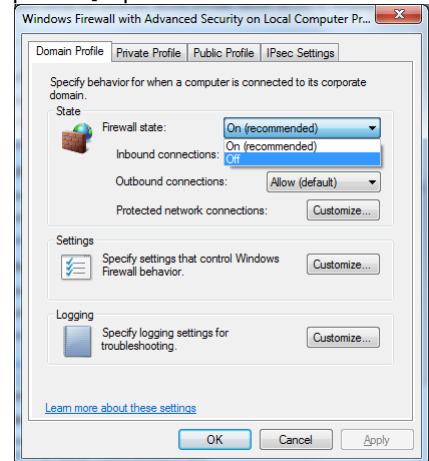
[1] From the [Start] menu, open [Control Panel] and click [System and Security] and then click [Administrative Tool]. Next, double-click [Windows Firewall with Advanced Security].

=> [Windows Firewall with Advanced Security] opens.



[2] Click [Windows Firewall Properties].

=> [Windows Firewall with Advanced Security on Local Computer Properties] opens.



[3] Click [Domain Profile] and set [Firewall state] to Off.

[4] Click [Private Profile] and set [Firewall state] to Off.

[5] Click [Public Profile] and set [Firewall state] to Off.

[6] Click [OK].

=> [Windows Firewall with Advanced Security on Local Computer Properties] closes.

[7] Close [Windows Firewall with Advanced Security].

IV-14. IIS Installation

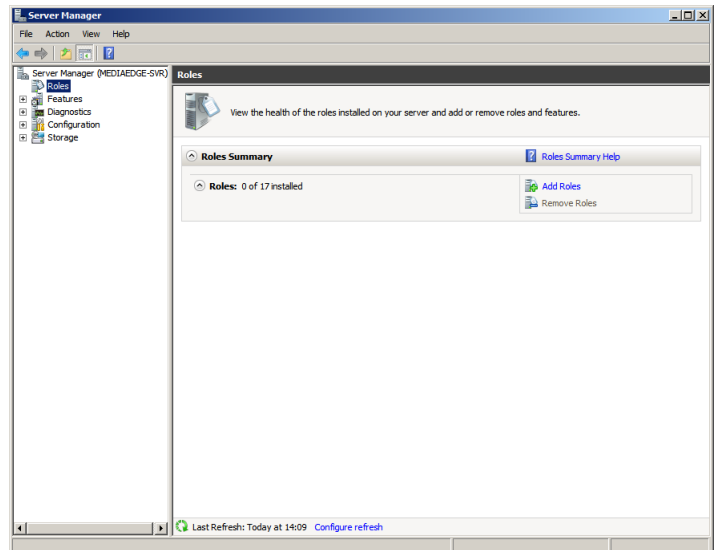
This section describes the procedure for installing IIS (Internet Information Service) on each operating system manually.

* Installer (version 1.60 or later) sets IIS during installation.

IV-14-1. Windows Server 2008 R2

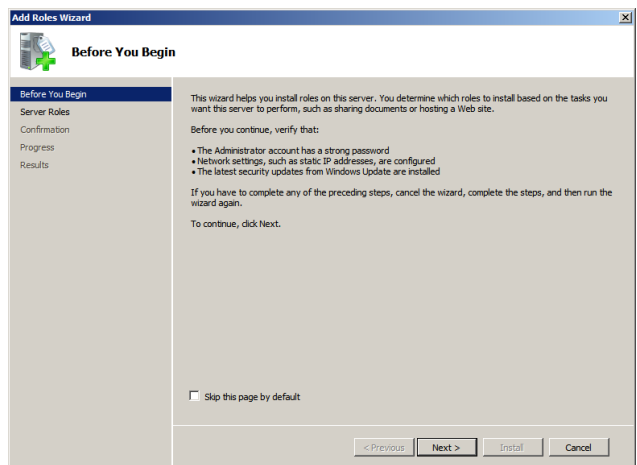
[1] From the [Start] menu, open [Control Panel] and click [System and Security] and then click [Administrative Tools]. Next, double-click [Server Manager].

=> [Server Manager] opens.



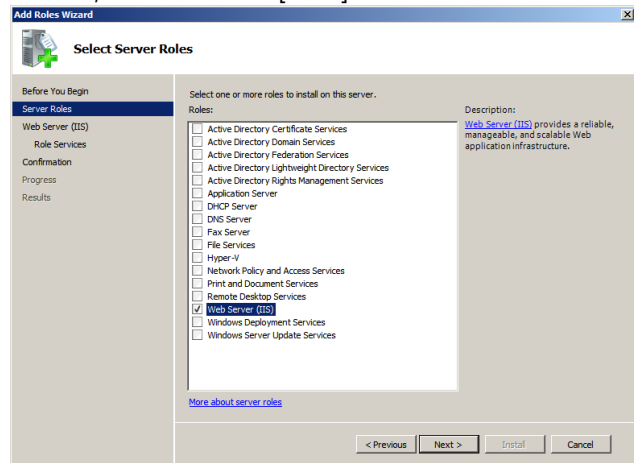
[2] Click [Roles] from the tree. Next, click [Add Roles].

=> [Add Roles Wizard] opens.



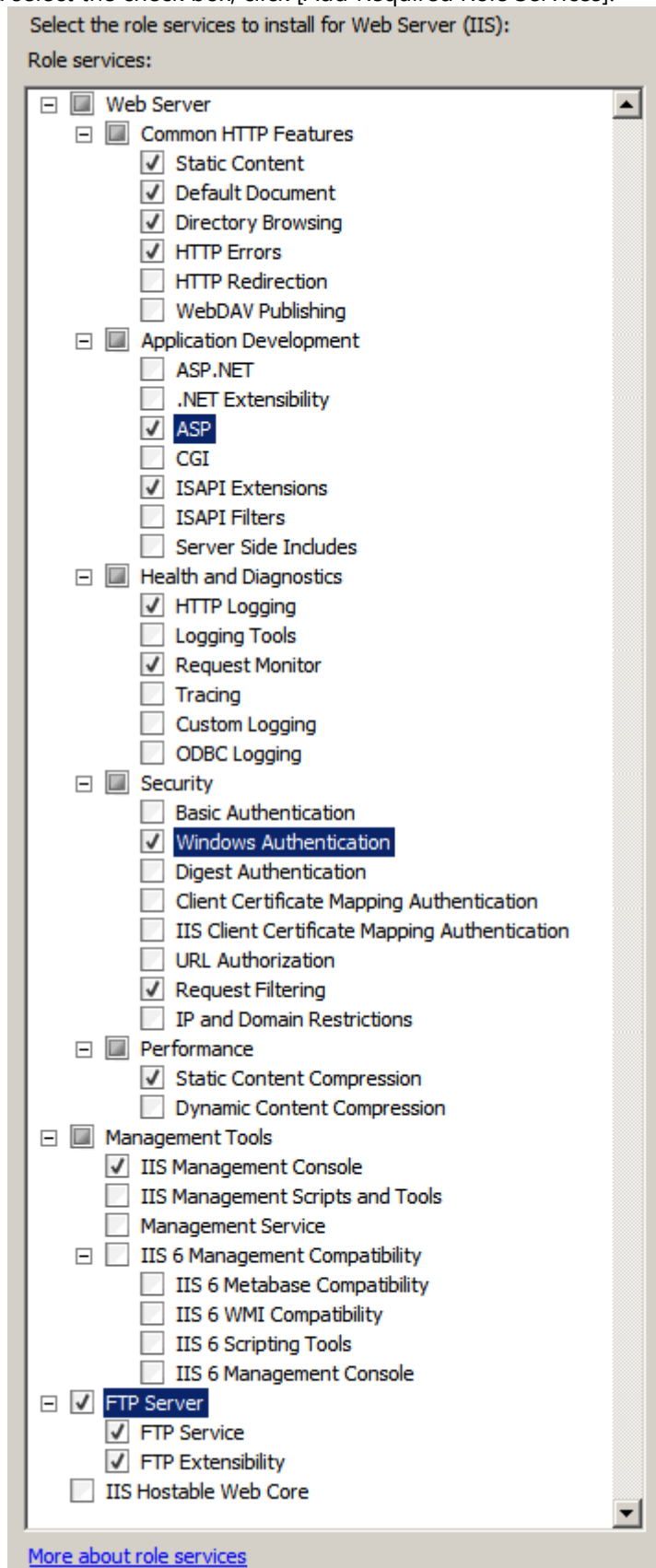
[3] Click [Next].

[4] In [Server Roles], select the [Web Server (IIS)] check box, and then click [Next].



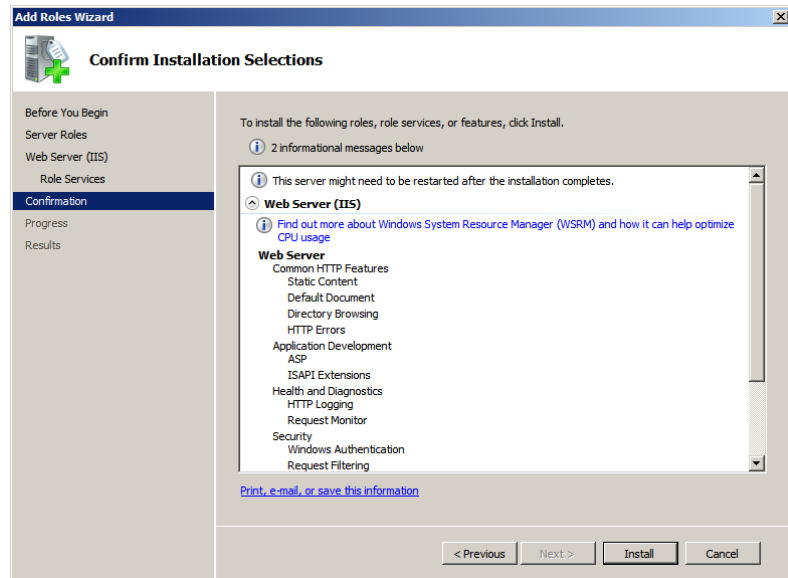
[5] In [Role Services], select the [AP.NET], [ASP], [Basic Authentication], [Windows Authentication] and [FTP Server] check boxes, and then click [Next]

If a confirmation message appears when you select the check box, click [Add Required Role Services].

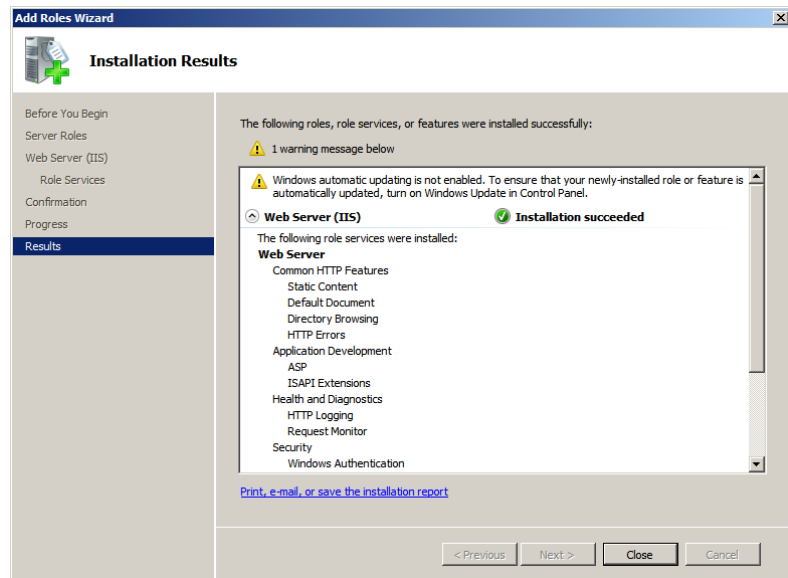


[6] Click [Install].

=> The installation starts.



[7] Click [Close].



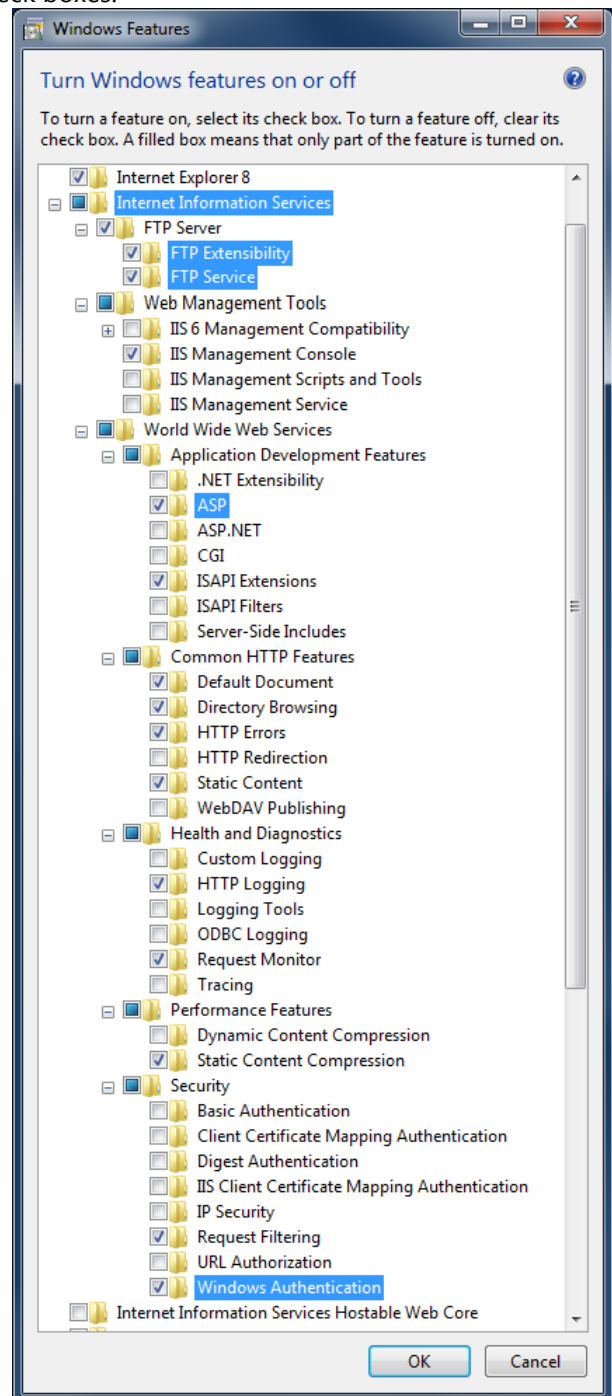
[8] Close [Server Manager].

IV-14-2. Windows 7

[1] From the [Start] menu, open [Control Panel]. Next, click [Programs], and then click [Turn Windows features on or off].

=> [Windows Features] opens.

[2] Select the [Internet Information Services] check box. Next, in the [Internet Information Services] tree, select the [FTP Extensibility], [FTP Service], [IIS Management Console], [IIS Management Scripts and Tools], [IIS Management Service], [ASP], [ASP.NET], [Default Document], [Directory Browsing], [HTTP Errors], [HTTP Redirection], [Static Content], [Basic Authentication] and [Windows Authentication] check boxes. In addition, select the [Windows Process Activation Service] and the subnodes; [.NET Environment], [Configuration APIs], [Process Model] check boxes.



[3] Click [OK].

=> The installation starts.

IV-15. FTP Server Settings

This section describes the procedure for setting the FTP server on each operating system.

* Installer (version 1.60 or later) sets FTP during installation if automatic creation has selected.

IV-15-1. Windows Server 2008 R2

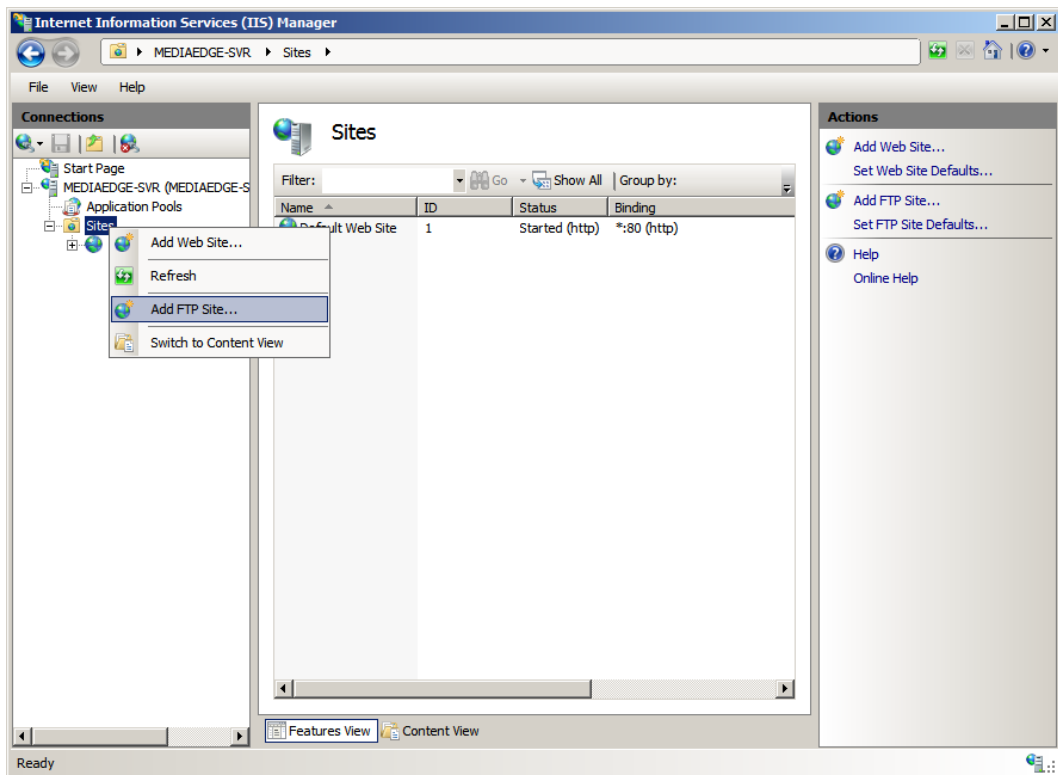
[1] From the [Start] menu, open [Control Panel] and click [System and Security] and then click [Administrative Tools]. Next, double-click [Internet Information Services (IIS) Manager].

=> [Internet Information Services (IIS) Manager] opens.

[2] From the tree, display
[MEDIAEDGE-SVR(MEDIAEDGE-SVR\Administrator)]->[Sites].

Next, right-click [Sites], and click [Add FTP Site].

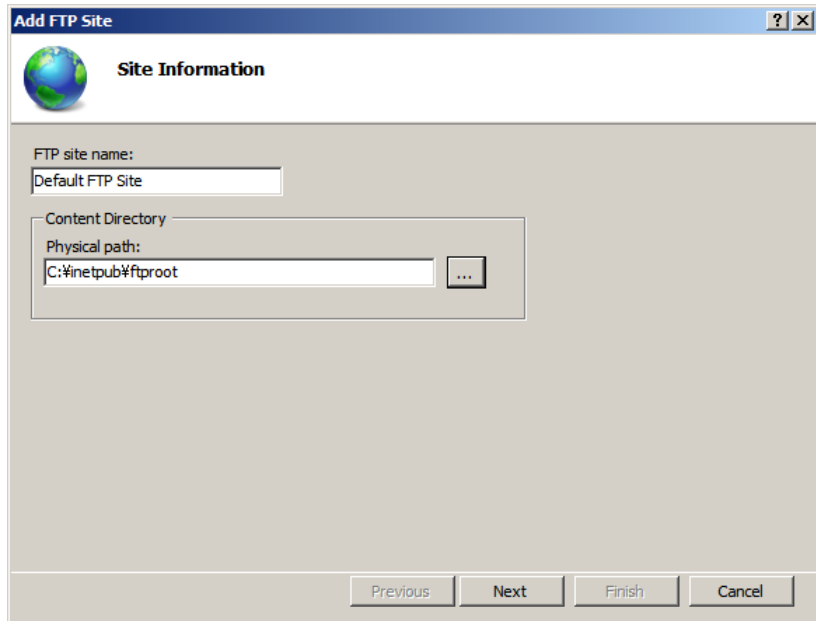
=> [Add FTP Site] opens.



[3] Set [FTP site name] and [Physical path], and then click [Next].

FTP site name Default FTP Site

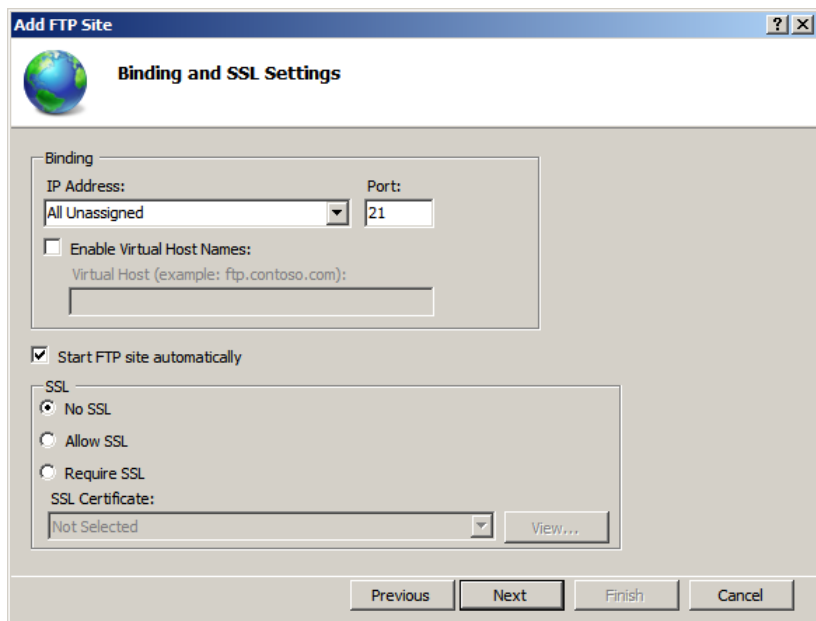
Physical path C:\inetpub\ftproot



The screenshot shows the 'Add FTP Site' dialog box with the 'Site Information' tab selected. The 'FTP site name' field contains 'Default FTP Site'. The 'Content Directory' section shows the 'Physical path' as 'C:\inetpub\ftproot'. At the bottom, there are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'.

[4] Set [SSL] and click [Next].

SSL : No SSL



The screenshot shows the 'Add FTP Site' dialog box with the 'Binding and SSL Settings' tab selected. In the 'Binding' section, 'IP Address' is set to 'All Unassigned' and 'Port' is '21'. The 'Enable Virtual Host Names' checkbox is unchecked. In the 'SSL' section, the 'No SSL' radio button is selected. The 'Start FTP site automatically' checkbox is checked. At the bottom, there are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'.

To encrypt transfer

* If you would like to encrypt transfer by SSL, check the [Allow SSL] or [Require SSL] box and select appropriate [SSL Certificate].

In advance, you must get legal [SSL Certificate] from Certificate Authority (CA) and register it to IIS or create a [self-signed certificate].

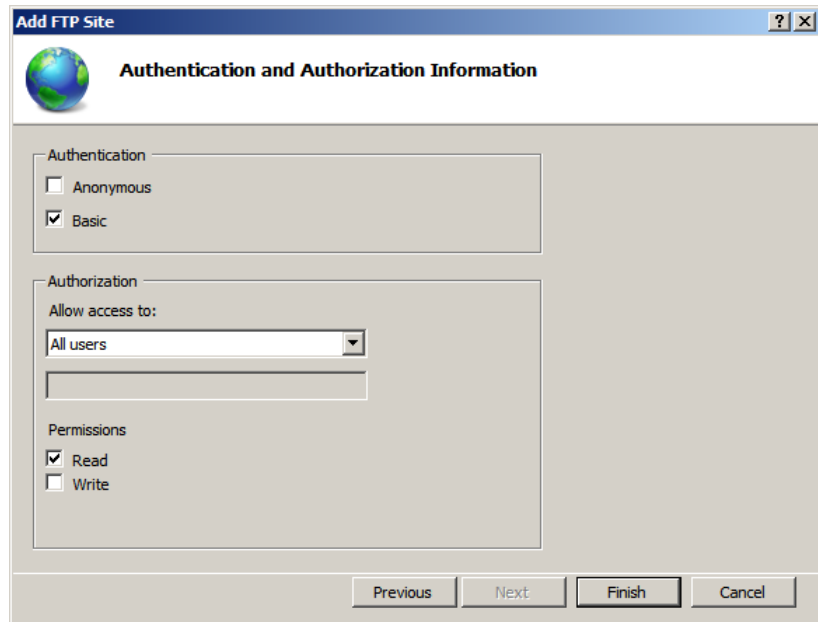
About [Self-signed certificate], please see [IV-16. How to create a self-signed certificate]

[5] Set [Authentication], [Allow access to] and [Permissions], and then click [Finish].

Authentication Basic

Allow access to All users

Permissions Read



[6] From the tree, right-click [Default FTP Site], and then click [Add Virtual Directory].

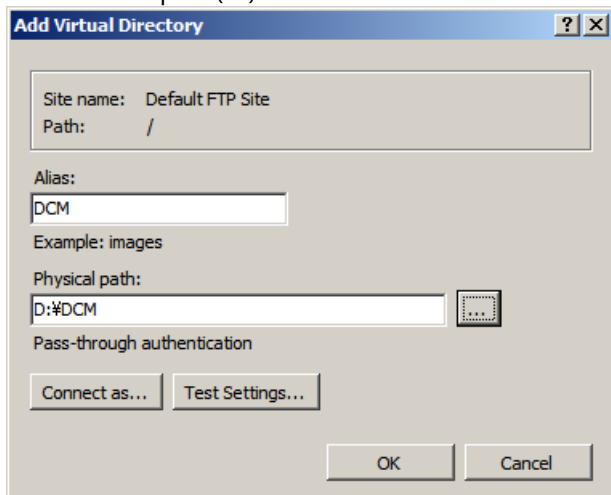
=> [Add Virtual Directory] opens.

[7] Set [Alias] and [Physical path], and then click [OK].

Alias DCM (*1)

Physical path D:\DCM

Because all the content files that are handled with Display Content Manager are uploaded to this [Physical path], create DCM folder in a drive that has a lot of free space(*2).

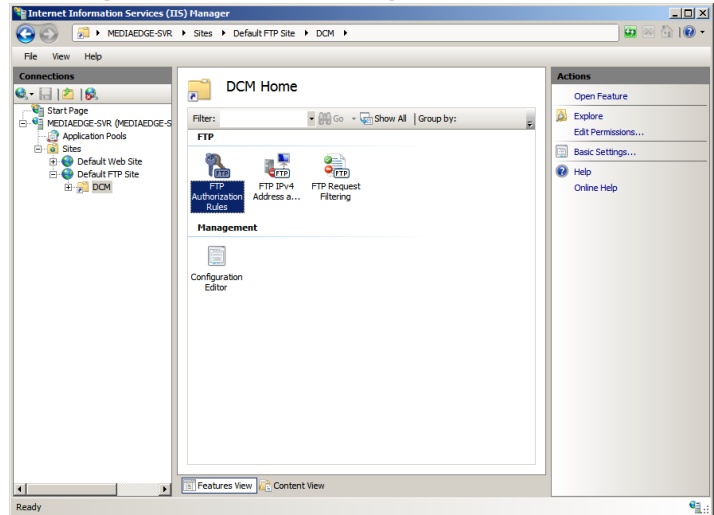


*1: [Alias] is used as part of the URI when accessing the FTP.

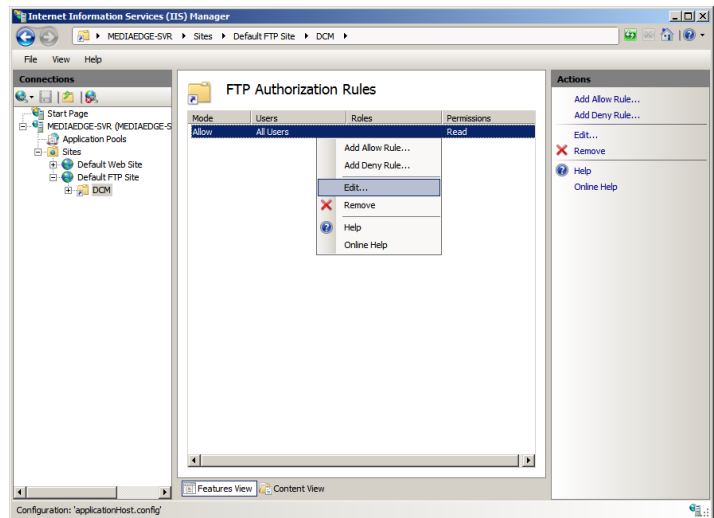
ftp://server name/alias/

*2: When installing the FTP server on the same computer as the various functions of Display Content Manager (DCM application, DCM server, DCM add-on for SVS), you can save disk space by setting the same folder in p.108 [III-5 Display Content Manager Installation].

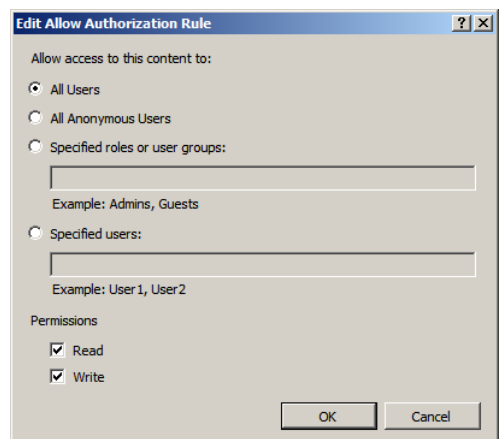
[8] From the tree, click [DCM], and then double-click [FTP Authorization Rules].



[9] Right-click [All Users], and click [Edit].



[10] Select the [Read] and [Write] check boxes, and click [OK].



[11] Close [Internet Information Services (IIS) Manager].

IV-15-2. Windows 7

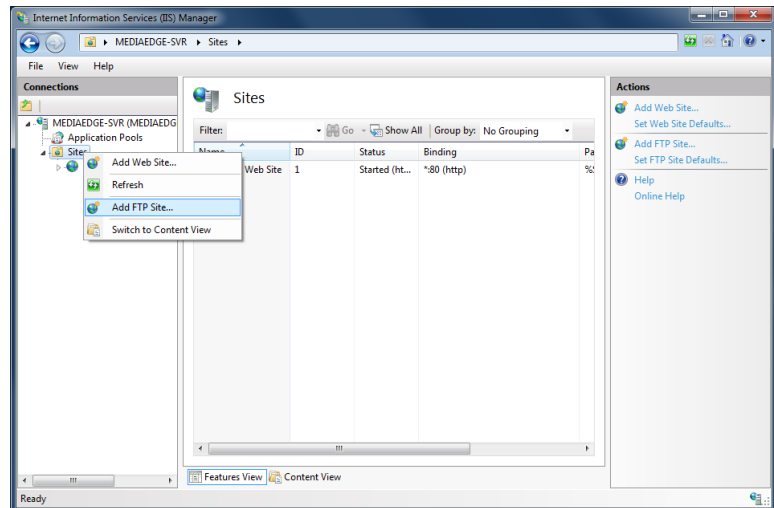
[1] From the [Start] menu, open [Control Panel] and click [System and Security] and then click [Administrative Tools]. Next, double-click [Internet Information Services (IIS) Manager].

=> [Internet Information Services (IIS) Manager] opens.

[2] From the tree, display [MEDIAEDGE-SVR(MEDIAEDGE-SVR\Administrator)]->[Sites].

Next, right-click [Sites], and click [Add FTP Site].

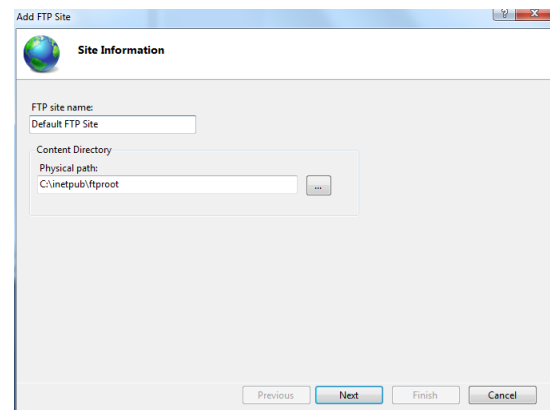
=> [Add FTP Site] opens.



[3] Set [FTP site name] and [Physical path], and then click [Next].

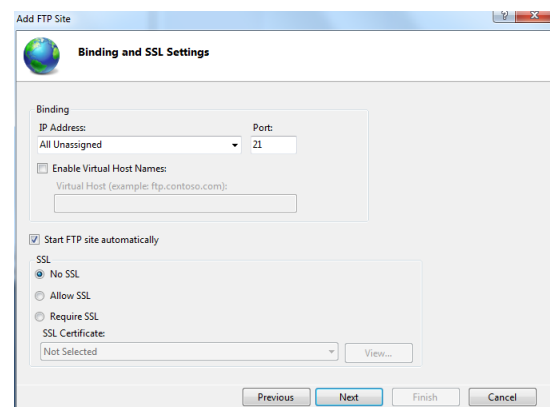
FTP site name Default FTP Site

Physical path C:\inetpub\ftproot



[4] Set [SSL] and click [Next].

SSL : No SSL



To encrypt transfer

If you would like to encrypt transfer by SSL, check the [Allow SSL] or [Require SSL] box and select appropriate [SSL Certificate].

In advance, you must get legal [SSL Certificate] from Certificate Authority (CA) and register it to IIS or create a [self-signed certificate].

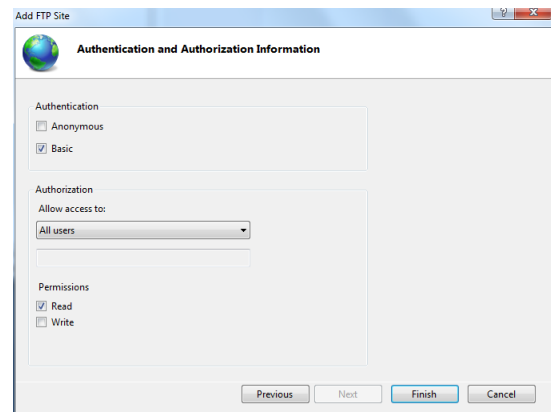
About [Self-signed certificate], please see [IV-16. How to create a self-signed certificate]

[5] Set [Authentication], [Allow access to] and [Permissions], and then click [Finish].

Authentication Basic

Allow access to All users

Permissions Read



[6] From the tree, right-click [Default FTP Site], and then click [Add Virtual Directory].

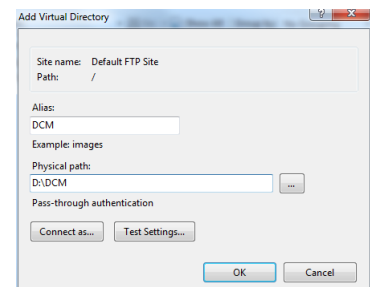
=> [Add Virtual Directory] opens.

[7] Set [Alias] and [Physical path], and then click [OK].

Alias DCM (*7)

Physical path D:\DCM

Because all the content files that are handled with Display Content Manager are uploaded to this [Physical path], create DCM folder in a drive that has a lot of free space(*8).

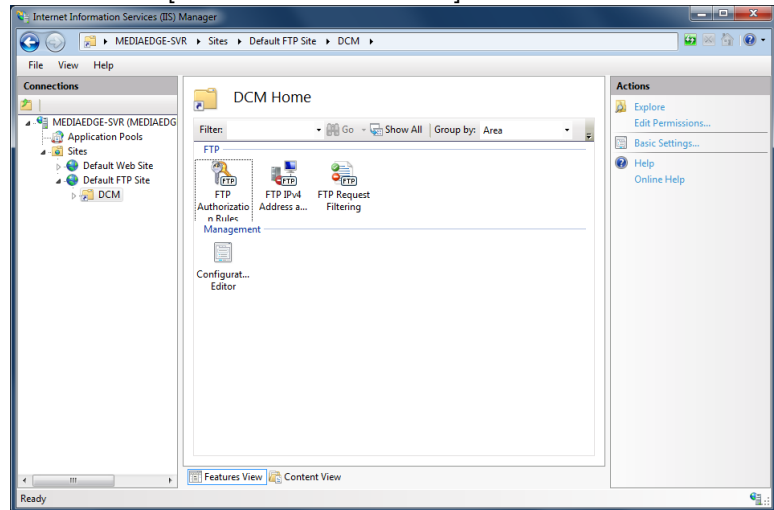


*7: [Alias] is used as part of the URI when accessing the FTP.

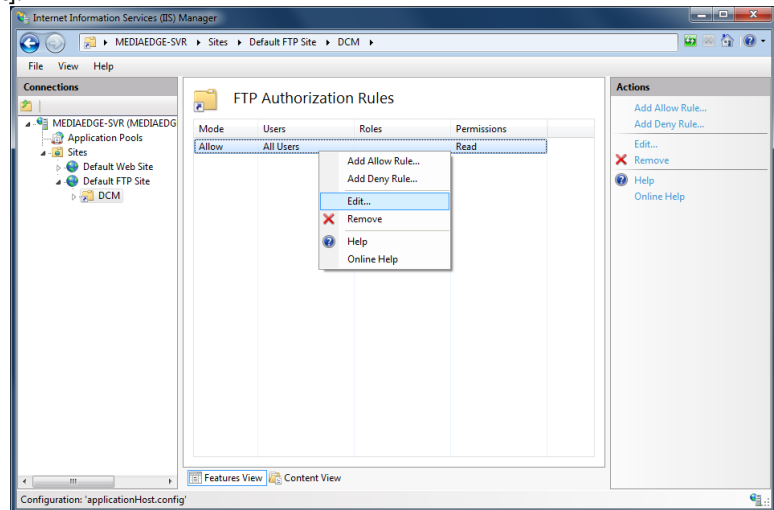
ftp://server name/alias/

*8: When installing the FTP server on the same computer as the various functions of Display Content Manager (DCM application, DCM server, DCM add-on for SVS), you can save disk space by setting the same folder in [II-5 Display Content Manager Installation].

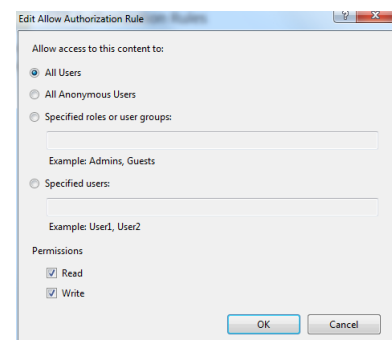
[8] From the tree, click [DCM], and then double-click [FTP Authorization Rules].



[9] Right-click [All Users], and click [Edit].



[10] Select the [Read] and [Write] check boxes, and click [OK].



[11] Close [Internet Information Services (IIS) Manager].

IV-16. How to create a self-signed certificate

The Web server and FTP server included in IIS 7.0 or later can encrypt transfer using the SSL with [SSL certificate]. This section describes how to create a [self-signed certificate].

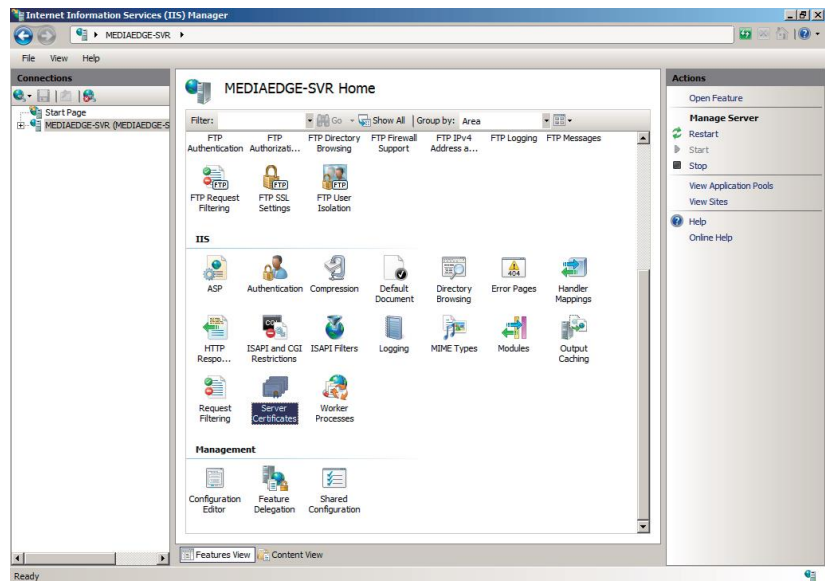
* Installer (version 1.70 or later) automatically create self-signed certificate during installation.
(Name : MEDIAEDGE-DCM Certificate, Term: 10 years)

About security strength of self-signed certificate

A self-signed certificate is less secure than CA-signed certificates (CA: Certificate Authority). Please use a self-signed certificate for simplified encrypted transfer only.

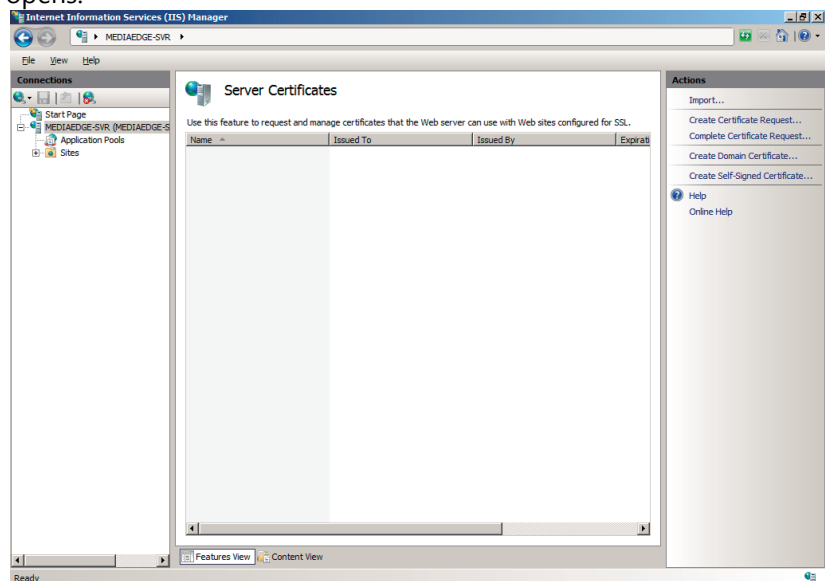
[1] Open [Internet Information Service (IIS) Manager].

[2] From the tree, display [MEDIAEDGE-SVR(MEDIAEDGE\Administrator)], and then double-click [Server Certificates].

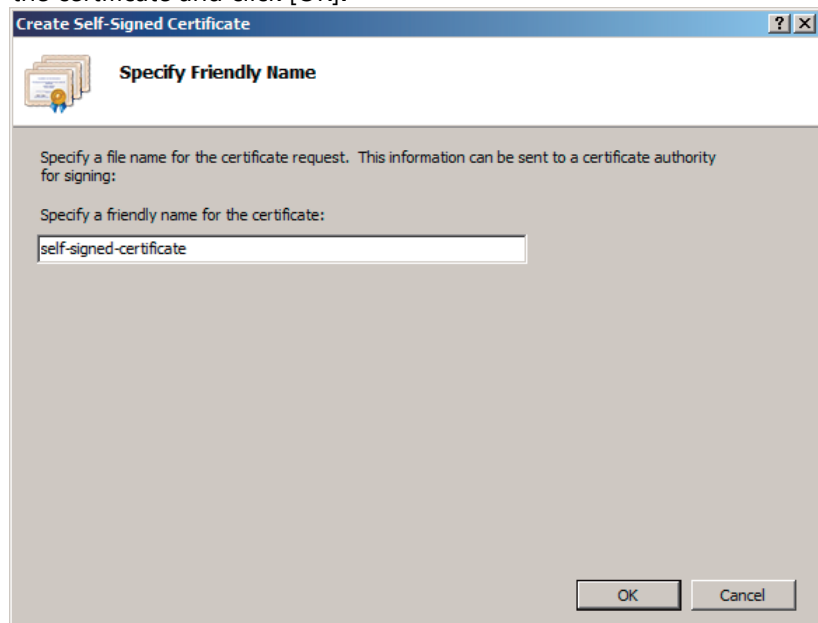


[3] Click [Create Self-Signed Certificate...] on the right-pane [Actions].

=> [Create Self-Signed Certificate] opens.



[4] Enter arbitrary friendly name for the certificate and click [OK].



V. Appendix

V-1. Restrictions

V-1-1. DCM Installer specifications and restrictions

Folder Name

Reserved names in Windows (MS-DOS device names) can not be used for installation folder and content folder.

Cases) CON, PRN, COM1, . . .

For details, please see the following page.

<http://support.microsoft.com/kb/74496/en-us>

V-1-2. DCM console specifications and usage restrictions

- Layouts
 - The size of layouts for STB and HDMA is fixed at 1920*1080 dots(*1).
 - Layouts for SWT can be set to any size from a minimum of 480*480 dots to a maximum of 1920*1920 dots.
 - The total number of regions that can be placed in a layout is 20.
 - ✧ The number of video regions that can be placed in an STB or HDMA layout is 1.
 - ✧ The number of video regions that can be placed in an SWT layout is 4.

*1: STB and HDMA are designed so that content other than video content (still images, tickers, FLASH, HTML) is handled in 960*540 dots and doubled in size both horizontally and vertically.
- Playlists
 - The length of a playlist can be specified from the shortest value of 15 seconds to the longest value of 23 hours, 59 minutes and 59 seconds.
 - Keep the number of components that are registered for one playlist to less than 1000.
 - ✧ Although operation is possible with more than 1000 components registered, it takes time to start playback because of the load. Where possible, keep registrations to less than 1000 items.
- Schedules
 - The length of a program can be specified from the shortest value of 15 seconds to the longest value of 23 hours, 59 minutes and 59 seconds.
 - Keep the number of programs that are registered for one day to less than 1000.
 - ✧ Although operation is possible with more than 1000 items registered, schedule updates may take a long time or the operation of the storage type playback clients may slow down. Where possible, keep registrations to less than 1000 items.
 - Keep the number of command programs that are registered for one day to less than 100.
 - ✧ Although operation is possible with more than 100 items registered, schedule updates may take a long time or the operation of the storage type playback clients may slow down. Where possible, keep registrations to less than 100 items.

- Updates
 - Update operation, number of days + 1 day files are transferred. (Example: If set 9 days and then an update on August 12, it transferred the files of 10 days from August 11 through August 20.)
 - ✧ Please adjust the number of days, to meet less than 10,000 of number of transferring programs. (For the ME-SVS server, less than 100,000)
 - ✧ Please adjust the number of days, so that the being transferred file size is smaller than the capacity of destination disk.
 - Two update methods are available, manual update and automatic update.
 - With automatic update, you can specify the approximate update length to perform file transfer at a slow speed.
 - A manual update can be performed from both the schedule window and the target window.
 - ✧ In the schedule window, start the update by specifying the channel to update. The update is performed for all the groups of MEDIAEDGE servers and storage type playback clients that are played back by the specified channel.
 - ✧ In the target window, start the update by directly specifying the groups of MEDIAEDGE servers and storage type playback clients to update.

V-1-3. Usage restrictions for multiple DCM consoles

If you work with multiple DCM consoles running at the same time in a single DCM system, data inconsistencies may occur. If multiple operators are working at the same time on multiple operation PCs, make sure that the same layout, playlist or channel is not edited at the same time. Because the DCM console does not have a function for detecting whether other DCM consoles are being used, care must be taken to ensure that operators do not perform editing at the same time.

V-1-4. Region overlapping sequence

The depth ordering (Z-order) is determined by the region number that is specified in the layout window of the DCM console. Usually, the regions are displayed in the specified order, but some playback clients ignore this specification.

STB and HDMA have the following restrictions.

- ✧ Video content is always at the back.
- ✧ Ticker content is always at the front.

SWT displays in the specified overlapping order.

V-1-5. Availability of simultaneous playback

Player	HD Video	Audio	4K Video	Images	Ticker	FLASH	Quick Time	HTML
ME-DEC	1 (*1)		--	1	1	--	--	1
STB4/HDMA-4100	1 (*1)		--	1	1	1 (*2)	--	4
HDSS-4K	4	4	1	16	2	4	4 (*3)	4
SWT4	4	4	--	16	2	4	4 (*3)	4

*1 The video and audio cannot be used simultaneously.

*2 To Flash7, Size 640x480

*3 Only stand-alone.

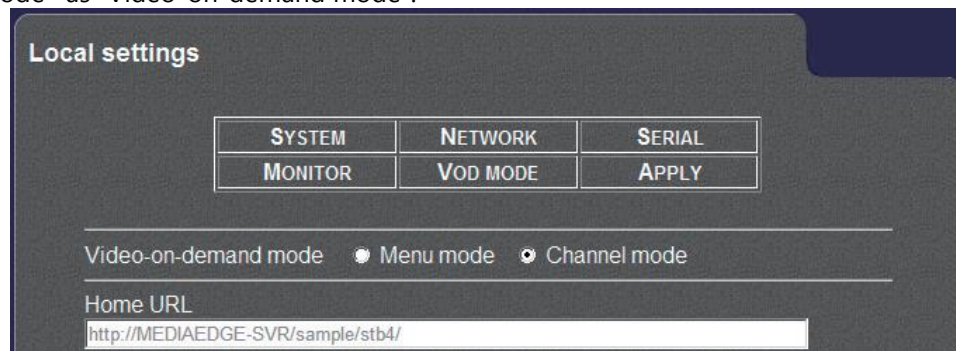
Content in excess of these restrictions can be laid out in the playlist window of the DCM console, but it will not actually play back. (For example, if you create a playlist for STB4H and place two or more ticker content items on a timeline so that they overlap, only one will be played back.)

V-2. How to start scheduled playback after restarting STB

V-2-1. Configuring the STB

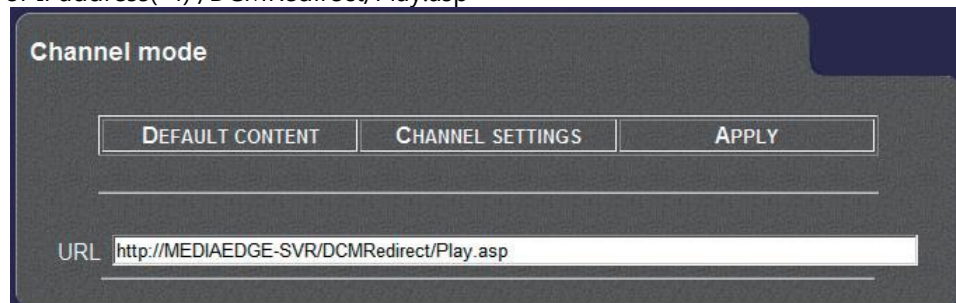
Please configure the STB settings with web console as below:

[1] Choose 'Channel mode ' as "Video-on-demand mode".



[2] Set following as default content URI.

=> http://ServerName or IPAddress(*4) /DCMRedirect/Play.asp

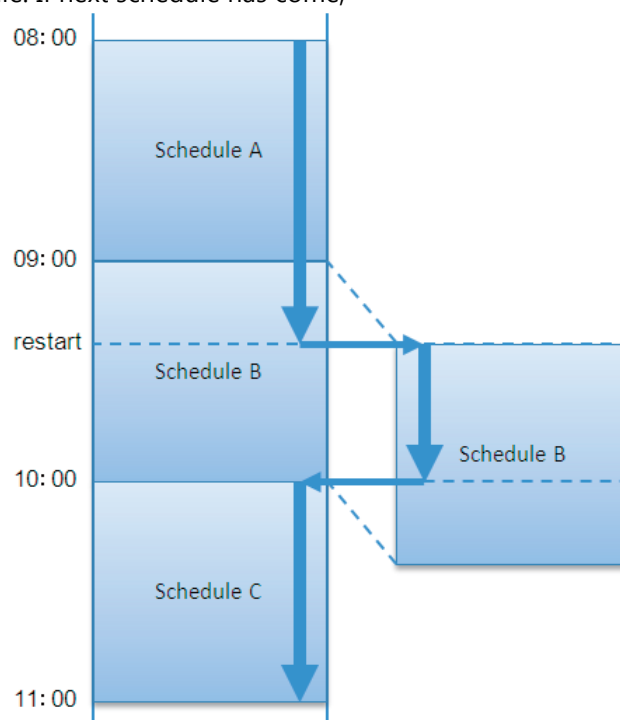


*4: MEDIAEDGE server on which DCM add-on for SVS has been installed.

[3] Scheduled playback will be started after restarting the STB.

V-2-2. Limitation as designed

Start position of playback is always top of the schedule. If next schedule has come,



MEDIAEDGE